VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

USRP B210 jako platforma pro vytváření prvků mobilní sítě

USRP B210 as Platform for Building Elements of Mobile Network

2014/2015 **Bc. Marek Kohut**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Bc. Marek Kohut**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T059 Mobilní technologie

Téma: USRP B210 jako platforma pro vytváření prvků mobilní sítě
USRP B210 as Platform for Building Elements of Mobile Network

Zásady pro vypracování:

Cílem diplomové práce je vytvoření eNodeB prvku mobilní sítě na HW platformě kitu USRP B210. Při realizaci bude diplomant využívat open-source projekt openLTE, kde probíhá otevřená implementace 3GPP LTE specifikace.

1. Vývoj mobilních sítí, principy a architektura.
2. Vlastnosti a využití USRP.
3. Návrh a realizace eNodeB prvku s využitím USRP.
4. Zhodnocení dosažených výsledků.

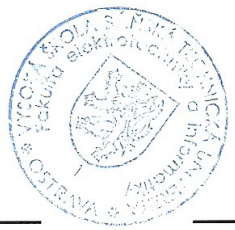
Seznam doporučené odborné literatury:

S. Sesia, I. Toufik, M. Baker. *LTE - The UMTS Long Term Evolution: From Theory to Practice*. John Wiley & Sons, 2009. DOI: 10.1002/9780470742891
A. Loula. *OpenBTS Installation and Configuration Guide*. 2009, Available on http://gnuradio.org/redmine/attachments/139/OpenBTS_Guide_En_v0.1.pdf.
M. Iedema. *Getting Started with OpenBTS*. O'Reilly, publishing scheduled on December 2014.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **doc. Ing. Miroslav Vozňák, Ph.D.**

Datum zadání: 01.09.2014
Datum odevzdání: 07.05.2015



doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

Dne: *4.5.2015*

.....
podpis studenta

Poděkování

Rád bych poděkoval doc. Ing. Miroslavu Vozňákovi, Ph.D. za odbornou pomoc, projevenou ochotu a konzultaci při vytváření této diplomové práce.

Abstrakt

Tato diplomová práce se zabývá vytvořením přístupového bodu vlastní LTE sítě, s využitím open-source projektu OpenLTE a softwarově definovaného rádia USRP B210. V textu jsou také popisovány veškeré závislosti, které jsou k vytvoření vlastního přístupového bodu LTE eNodeB pomoci OpenLTE zapotřebí. Práce dále obsahuje konfiguraci jednotlivých prvků ve vlastní síti a ukázku možností využití přístupového bodu, které nabízí aktuální verze projektu OpenLTE. Na závěr jsou dosažené výsledky z experimentálního provozu vlastního přístupového bodu zhodnoceny a jsou nastíněny možnosti využití tohoto projektu.

Klíčová slova

LTE, OpenLTE, USRP B210, eNodeB.

Abstract

This diploma thesis describes creation of access point of own LTE network with usage of open-source project OpenLTE and software defined radio USRP B210. All of the requirements for creating own LTE eNodeB access point are also stated in this text. This thesis also includes configuration of all elements, that are used in own network and description of possible usage of OpenLTE network in its current version. The results, obtained from the experimental operation of access point, as well as possibilities of this project for practical use, are reviewed in the last part of this thesis.

Keywords

LTE, OpenLTE, USRP B210, eNodeB.

Seznam použitých zkratek

Zkratka	Anglický význam	Český význam
LTE	Long Term Evolution	Technologie pro vysokorychlostní přenos dat v mobilních sítích
OpenLTE	Open Long Term Evolution	Projekt zabývající se implementaci vlastního LTE přístupového bodu
USRP	Universal Software Radio Peripheral	Softwarově definované rádio
USIM	Universal SIM	Nový typ SIM karty
UHD	USRP Hardware Driver	Ovladač pro komunikaci mezi USRP a PC
IMSI	International mobile subscriber identity	Identifikátor SIM karty
UE	User equipment	Koncové mobilní zařízení
eNodeB	Evolved Node B	Základnová stanice pro nové typy mobilních sítí
UMTS	Universal Mobile Telecommunication System	další stupeň vývoje GSM sítí v rámci 3GPP
VoLTE	Voice over LTE	technologie umožňující přenášet hlasové hovory přes sítě LTE

Obsah

1 Úvod

Život bez mobilních technologií si dnes už jen těžko dokážeme představit. Staly se součástí našeho každodenního života a to nejen kvůli hovorům a SMS zprávám, ale také kvůli multimediální zábavě a přístupu k internetu. Právě rychlost mobilního připojení k internetu zaznamenala během několika posledních let výrazných změn v rychlosti díky vývoji nových technologií, jako je například LTE. V současné době se vyskytuje několik projektů, zaměřujících se na implementaci vlastního LTE přístupového bodu a tak nabízí možnost vyzkoušet si, jak vlastně taková síť funguje. Jedním z těchto projektů je i OpenLTE.

V této práci se budu zabývat postupem, jakým je možné vytvořit vlastní přístupový bod eNodeB s využitím softwarově definovaného rádia USRP B210 od firmy ETTUS a výše zmíněného softwaru OpenLTE. Uvedu zde všechny náležitosti, které je třeba splnit při vytváření takovéhoto přístupového bodu, a následně zhodnotím výsledky, kterých během experimentálního provozu dosáhnu.

Samotná práce je rozdělená do čtyř částí. V první se budu zabývat vývojem a historií jednotlivých mobilních sítí, od první do čtvrté generace, z hlediska jejich principů a architektury. Ve druhé pak popíši rádiovou periférii USRP, její architekturu a využití. Třetí část pak nabídne popis samotného vytvoření vlastního přístupového bodu eNodeB a testování dostupné funkcionality s reálným mobilním telefonem. Ve čtvrté části pak dosažené výsledky zhodnotím a pokusím se navrhnout reálné využití projektu OpenLTE.

2 Vývoj mobilních sítí, principy a architektura.

2.1 Sítě nulté generace (0G-0.5G)

Za vůbec prvního předchůdce dnešní mobilní telefonie můžeme považovat služby dostupné téměř ihned po skončení druhé světové války. Tato technologie ovšem zatím nevyužívala buňky – prostor, v jehož středu se nachází základnová stanice zprostředkující komunikaci s koncovými zařízeními. O samotné spojení mezi dvěma body se staral mobilní operátor, který přiřadil hovor k jednomu, z ne mnoha v té době dostupných, kanálů. Protože se zde bavíme o předchůdcích první generace, která využívala ke svému fungování buňkový prostor, je tato generace nazvána tzv. nultou generací mobilních sítí. V této generaci byly využívány technologie jako Push to Talk, MTS (Mobile Telephone System), IMTS (Improved Mobile Telephone system), AMTS (Advanced Mobile Telephone system), OLT (Norská zkratka pro mobilní telefonii) nebo MTD (Švédská zkratka pro mobilní telefonii). Od předchozích mobilních systémů se lišily tím, že služba byla dostupná jako komerční služba, která byla součástí veřejného systému přepínané telefonní sítě namísto uzavřené sítě, která byla používána například pro policejní a jiné záchranné složky nebo taxi službu.[1]

Mobilní zařízení, která se používala v této generaci, byla zabudována v automobilech nebo nákladních autech ale vyskytovala se i "přenosná" osobní zařízení velkého rozměru, která byla dodávána v kufřících. V automobilech byl transceiver takového zařízení zabudován většinou v úschovném prostoru a byla k němu připevněna tzv. hlava, která obsahovala hlavní ovládací prvky jako displej, sluchátko nebo vytáčecí zařízení. Tato zařízení bylo možné získat přes telefonní společnosti (WCC, RCC, Bell System).[1,2]

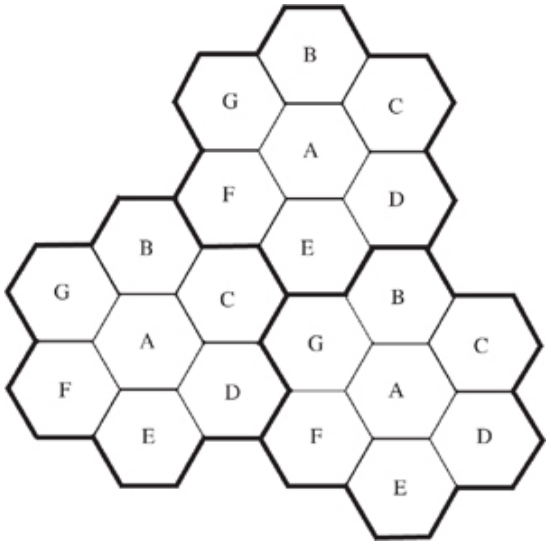
Je nutné také poznamenat problémy, které byly spojovány s nultou generací mobilních sítí. Jedním z nich byla obrovská vytíženost kanálů z důvodu využití velké šířky pásma, s kterou tato generace pracovala. V Americe se počet kanálů na celou zemi v počátcích pohyboval okolo 54. To s kombinací s nemožností opakovaní stejné frekvence, jak je tomu u buňkových sítí, představovalo největší problém této generace. Navíc, poptávka po mobilním telefonování byla tak obrovská, že v roce 1976 byla až jedna třetina zákazníků zařazena na čekací listinu pro získání přístroje a přístupu do sítě, čekací lhůta se pohybovala kolem pěti let.[1,2]

Jako první byla tato technologie komerčně nasazena v roce 1971 ve Finsku pod názvem ARP (Autoradiopuhelin), za zmínku také stojí nasazení v Německu v roce 1972. Německo nasadilo systém ke komerčnímu provozu pod názvem B-Netz jako druhé, ovšem zajistilo si prvenství v tom, že již nebylo potřeba lidských operátorů pro spojování hovorů, ale vše probíhalo automaticky.[1,2]

2.2 Sítě první generace (1G)

Jako první generaci označujeme analogový telekomunikační standard pro bezdrátovou mobilní telefonii, který byl představen v osmdesátých letech dvacátého století a přetrval až do doby, kdy byl nahrazen telekomunikačními sítěmi druhé generace. Zřejmě největším rozdílem právě mezi těmito dvěma generacemi je použitý rádiový signál. Zatímco u 1G je signál analogový, u 2G už je digitální. A i přestože oba systémy používají digitální signalizaci pro připojení radiové základny ke zbytku telefonního systému, je zde rozdíl v tom, jak je dále zpracován samotný hovor. U systémů 2G je hlas převáděn do digitálního signálu, u systémů první generace je pouze modulován do vyšších frekvencí, většinou ke 150MHz a výše.[3]

Tato generace jako první přišla s myšlenkou rozložení určité geografické oblasti do tzv. buněk – oblastí velkých přibližně 10–25 kilometrů a každá buňka je spravována samostatnou základnovou stanicí. Buňky jsou rozlohou poměrně malé a tak je možné využít opakování stejné, již jednou využité frekvence v blízkých (ovšem ne přímo přilehlých) buňkách jak je znázorněno na obr. 2.1, kde je patrné schéma tří svazků buněk, kdy každá část označená stejným písmenem může využívat stejnou frekvenci. Tímto postupem je možné obsloužit v dané oblasti mnohem více uživatelů.[3]



Obrázek 2.1: *Rozložení stejných frekvencí v buňkách[4]*

2.2.1 AMPS

Ve srovnání s technologii IMTS z nulté generace, je možné pomoci technologie AMPS druhé generace obsloužit přibližně 5 až 10 krát více účastníků ve stejné oblasti o rozloze 150 kilometrů, pokud by se tato oblast rozdělila na dvacet menších buněk, ve kterých by bylo možné využít opakování frekvencí. Navíc, i z hlediska nákladů je výhodnější rozdělení velké oblasti do buněk, neboť tyto menší oblasti často potřebují ke svému správnému provozu méně výkonné a levnější zařízení, která slouží k příjmu a odesílání informací.[2,3]

Samotná technologie AMPS, která vznikla v osmdesátých letech, byla charakterizována jako analogový rádiový mobilní systém využívající frekvenční modulace. Využitou metodou pro přístup k médiu bylo frekvenční dělení pásma (FDMA) s 30 kHz odstupem kanálů a 70 MHz šířkou pásma (824 MHz-894 MHz). Tato technologie je považována za vůbec první systém buňkových sítí, která byla využita pro komerční účely. Přetrvala až do začátku devadesátých let 20. století, kdy byla nahrazena sítěmi druhé generace. Tato technologie byla využita hlavně v Americe, odkud pochází a později se rozšířila i do Izraele nebo Austrálie. V Americe byla pro tuto technologii vyhrazena dvě 25 MHz pásma, jedno pro komunikaci základnové stanice směrem k mobilnímu zařízení a druhé pásmo pro opačnou komunikaci. Každý mobilní telefon byl vybaven 32 bitovým sériovým číslem a desítimístným telefonním číslem v paměti PROM takovéhoto zařízení. Přihlášení zařízení do sítě a sestavení hovoru probíhalo následovně: Po zapnutí se snaží telefon zaznamenat kontrolní signál vyslaný ze základnové stanice, základnové stanici s nejsilnějším signálem pošle své informace, které jsou dále postoupeny jako paket do MTS. Pokud chce uživatel sestavit hovor, jsou po zadání a odeslání požadovaného čísla na telefonu tyto informace zaslány do MTS, kde se kontroluje validita čísla a proběhne autorizace uživatele. MTS poté zajistí potřebné kanály pro sestavení spojení a pošle vyzváněcí signál do cílového telefonu. Pokud druhá strana odpoví, MTS sestaví hovorový okruh a začne zaznamenávat informace o délce hovoru a ostatních podrobnostech, které jsou dále třeba pro vyúčtování po ukončení hovoru. Po ukončení hovoru uvolní hovorový okruh i kanály které byly využity a dokončí vyúčtování.[3]

2.2.2 **NMT**

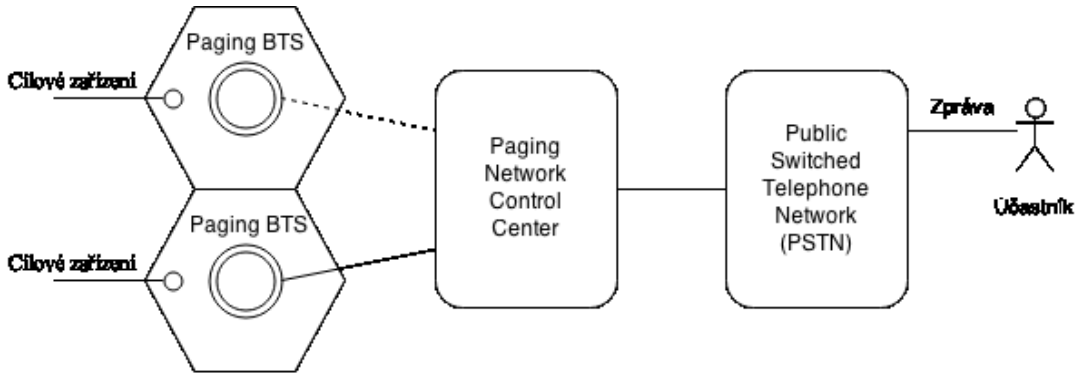
V roce 1981 pak byl spuštěn v Saudské Arábii, Norsku, Dánsku, Švédsku, Finsku a později i dalších státech, automatický systém mobilní telefonie, označovaný jako Nordic Mobile Telephone (NMT), pomoci kterého bylo možné vytvořit síť, která umožňovala provozovat mezinárodní roaming. Tato systém postupně nahradil již poměrně přetížené sítě ARP, MTD a OLT. Frekvenční pásmo, které NMT využívalo, bylo původně 450 MHz (NMT-450), později ovšem z důvodu potřeby zvýšení kapacity bylo v některých zemích využito i pásmo 900 MHz (NMT-900). Velikost buněk v MNT se pohybovala od 2 km do 30 km a nabízela plně funkční přepínání hovoru během změny polohy mobilního zařízení bez výpadku hovoru, tzv. handover. NMT také nabízela ještě před příchodem sítí 2G jednoduchou výměnu dat pomoci signalizačního kanálu – DMS nebo NMT-Text určenou pro přenos dat i textových zpráv. Dostupnost této služby byla ale velmi omezená jen na několik málo států, které NMT využívaly (Rusko, Polsko). Další možností, jak využít datový přenos bylo použití NMT Mobidigi, které pracovalo rychlostí 380 bps ovšem vyžadovalo externí zařízení. Pro signalizaci je v NMT využit hovor využit signalizační kanál, což lze rozpoznat pomoci charakteristického zvuku při handoveru. Pro modulaci je využita metoda FFSK a datová rychlost se pohybuje od 600 bps až po 1200 bps.[3]

2.2.3 Bezpečnost v sítích 1G

Z důvodu toho, že sítě první generace byly analogové, vyskytly se zde problémy s bezpečností. Téměř každý, kdo vlastnil rádiový přijímač, který byl schopný naslouchat na všech frekvencích, mohl odposlouchávat hovory, které na právě nastavené frekvenci probíhaly. Dále pak bylo možné s pomocí počítače zjistit 32 bitové sériové číslo zařízení a telefonní číslo účastníka, protože tyto informace byly do MTS zaslány jako pakety. Tak bylo možné vytvářet obrovské databáze čísel a následně je zneužít při reprogramování a přeprodávání telefonních přístrojů.[3]

2.2.4 Paging v sítích 1G

Pagingová síť je jednou z vůbec nejstarších bezdrátových technologií vůbec. Nabízí podporu jedno nebo obousměrného posílání krátkých zpráv, nebo poslechnutí krátkého hlasového záznamu, který byl na dané zařízení zaslán. Provozovatel provozující paging síť má k dispozici kontrolní středisko, které dostává žádosti o zaslání pagingové zprávy, které přicházejí od běžných telefonních přístrojů nebo jiných pagerů a tato kontrolní střediska je pak pomoci propojení s Paging BTS (spojení PNCC-Paging BTS může být jak bezdrátové, tak pomocí jiného pevného média) dále posílají k cílovým zařízením. V závislosti, zda je cílové zařízení schopno komunikovat jednostranně nebo oboustranně, je pak možné na příchozí zprávu reagovat nebo jí jen přijmout. V případě obousměrného zařízení je možné ihned odpovědět některou z předefinovaných zpráv nebo zaslat vlastní pagingovou textovou zprávu. Právě v této 1G generaci vznikl protokol POCSAG, který slouží pro přenos pagingových zpráv dodnes. Přenosové rychlosti se u těchto zařízení pohybovaly kolem 1200 bps. Provoz byl uskutečněn v pásmu 800 MHz. Masové rozšíření těchto technologií bylo zaznamenáno hlavně v Americe, kde dosahovalo pokrytí až 95% celého území Spojených států.[3]



Obrázek 2.2: *Architektura pagingové sítě[3]*

.

Výhody pagingových sítí spočívají hlavně v nízkých nákladech, dobrých možnostech pokrytí a poměrně jednoduché dostupnosti pro účastníka, který zprávu posílá (z jakéhokoliv telefonu). Některé z potíží, které se mohou v těchto sítích vyskytnout, jsou pomalé přenosové rychlosti, možná přetíženost sítě a žádná zpětná odezva při doručení zprávy, nepočítáme-li přímou odpověď účastníka, který zprávu obdržel.[3]

2.3 Sítě 2. generace (2G-2.75G)

Velká změna z pohledu mobilní telefonie proběhla na konci 80. let, kdy se začaly využívat pro přenos hovorů digitální přenosy a pomalu se začalo upouštět od analogových. Mezi nejdůležitější změny, které se objevily v druhé generaci a nechaly tak za sebou generaci první je lepší využití pásma, možnost šifrování digitálního signálu a nabídka pestré škály služeb i mimo samotné hovory, jakými jsou například přenos dat nebo možnost posílání krátkých textových zpráv (SMS). Zůstal zachován systém buňkových sítí, stejně jako to, že jako první, i druhá generace využívá digitální signalizace pro připojení rádiových stanic do zbytku telefonního systému. Významnými rozdíly mezi 1G a 2G tedy jsou:[2,3]

- Využití digitálních komunikačních kanálů namísto analogových
- Možnost využití šifrování, které zamezuje odposlouchávání hovorů
- Přistup ke kanálům – systémy 2G dovolují dynamické sdílení kanálů podle počtu aktivních účastníků
- 2G systémy umožňují využít detekci a opravu chyb při přenosu a zlepšit tak čistotu ve vnímaném zvuku
- 2G systémy, z důvodu využití digitalizace, dovolují přenos pomoci datových služeb

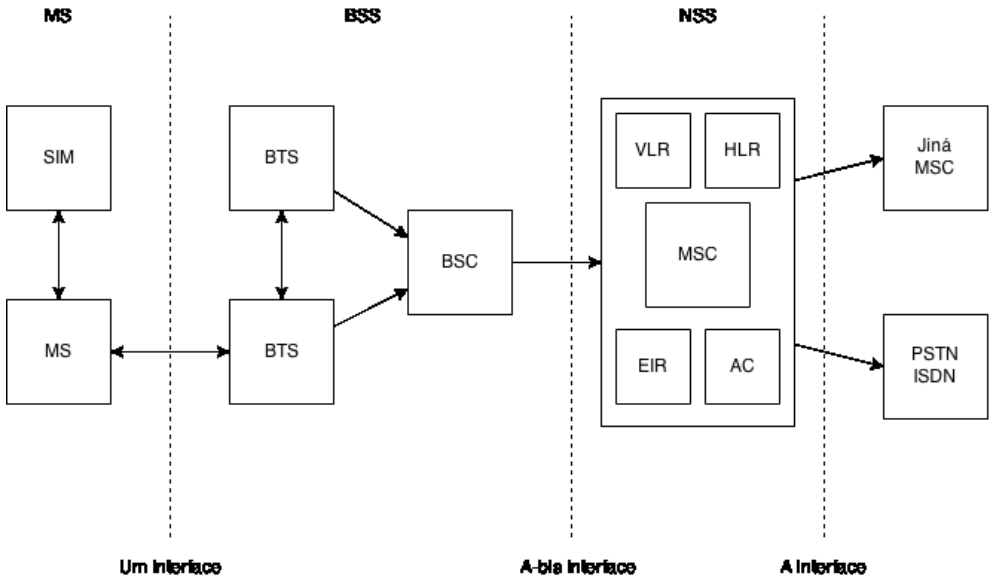
2.3.1 GSM (Global System for Mobile Communications)

GSM je označení pro zdaleka nejznámější technologii druhé generace vůbec. Tyto sítě si získaly zdaleka největší pozornost v Evropě a celkově se odhaduje, že ji využívá okolo pěti miliard uživatelů ve více než 200 zemích. Tyto sítě jsou schopny pracovat s rychlostí až 9.6 Kbps a jsou založeny na standardech definovaných institutem ETSI (European Telecommunications Standards Institute). Protože je GSM sytém vytvořen bez jakéhokoliv využití sítí předchozí generace, není s nimi zpětně kompatibilní. Jak už bylo uvedeno, je systém schopný dosáhnout rychlosti přenosu až 9.6 Kbps za použití 124 kanálů na buňku. Každý kanál pak zvládne obsloužit až 8 účastníků za využití TDMA. Některé z kanálů pak mohou sloužit také pro kontrolní signály pro mobilní zařízení, pomoci kterých je možné určit polohu nejbližší základnové stanice.[3]

GSM nenabízí jen možnost hovorů, ale také využití datových služeb, pro přístup k bezdrátovému připojení. Například je možné využít mobilní zařízení podporující GSM jako modem pro přístup k internetu, mailu apod. GSM také podporuje roaming mezi zeměmi Severní Ameriky a Evropy za předpokladu, že uživatel disponuje buď SIM kartou, nebo mobilním telefonem druhé země, z důvodu rozličných frekvencí. GSM je postavená na úzkopásmové TDMA technologii, kdy jsou frekvenční pásma rozdělena do tzv. timeslotů, kdy má každý z účastníků přístup do jednoho timeslotu v pravidelných intervalech.[2,3]

2.3.2 Architektura GSM

Architektura sítě GSM se skládá z několika vzájemně propojených rozhraní, jejichž schéma a popis je popsán níže.



Obrázek 2.3: *Blokové schéma architektury sítě GSM[5]*

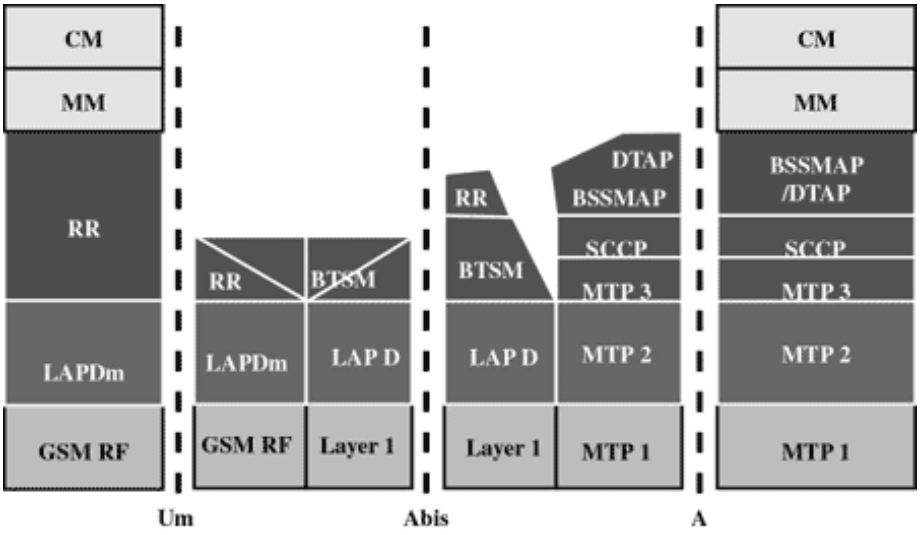
Mobilní stanice (MS): Představuje samotné uživatelské telekomunikační koncové zařízení, které komunikuje rádiově přes Um rozhraní se základnovou stanicí ve stejné buňce, ve které se nachází MS. MS se skládá z vlastního terminálu, jakým může být mobilní telefon nebo PDA a obsahuje zabudovaný rádiový transceiver, procesor pro zpracování digitálního signálu a SIM kartu.[3]

Base Station Subsystem (BSS): Skládá se z jedné nebo více základnových stanic (Base Transceiver Station – BTS) a jednoho Base Station Controller (BSC). Každá BTS definuje právě jednu buňku a skládá se z rádiové antény, rádiového transceiveru a tvoří spojení s BSC. BSC se stará o rezervaci rádiových frekvencí, handovery v rámci jednoho BSS a stará se o paging zprávy, které slouží k sestavení nebo ukončení hovoru s konkrétním MS.[3]

Mobile Switching Center (MSC): Hlavní centrum sítí GSM. Zprostředkovává spojení mezi buňkovými sítěmi a PSTN. Také se stará o přepojování hovorů mezi různými BSS, ověřuje uživatele a umožňuje celosvětový roaming. MSC se skládá z několika databázových prvků:

- Home Location Register (HLR) - ukládá informace o uživatelích kteří spadají do této HLR, také obsahuje informace o předplacených službách
- Visitor Location Register (VLR) - spravuje informace o uživatelích, kteří se fyzicky nachází v oblasti
- Authentication Center Database (AuC) - využívá se pro ověřování a obsahuje kopie tajných klíčů, které se používají při přihlášení do sítě a jsou uloženy na SIM kartě
- Equipment Identity Register Database (EIR) - registr mobilních zařízení v síti, kde je účastník identifikován podle IMEI čísla[3]

Mezi těmito klíčovými prvky GSM sítě je také přenášeno velké množství kontrolních zpráv. Tyto zprávy slouží pro podporu mobility a správu připojení. Na níže uvedeném obrázku, na kterém je zobrazena architektura sítě GSM z pohledu protokolů, je patrné, že můžeme tuto architekturu rozdělit podle klasicky do sedmi vrstev. Nižší vrstvy zde zajišťují přenos pomoci rádiového spojení (MS-BTS) nebo drátového (BTS-MSC). Vyšší vrstvy se pak starají o další specifické funkce.[3]



Obrázek 2.4: *Protokolová struktura v sítí GSM[5]*

- Connection Management (CM) - propojuje koncového uživatele (MS) s MSC nebo jiným koncovým uživatelem, nachází se na 6. vrstvě
- Mobility Management (MM) - zastřešuje operace související s určováním polohy a zabezpečením. Nachází se na 5. vrstvě

- Radio Resource Management (RR nebo RRM) - stará se o přiřazování a uvolňování kanálů a také o handovery. Nachází se na 3. vrstvě. V této vrstvě se také nachází protokoly, které jsou použity při komunikaci MS s BTS
- BTS Management (BTSM) - používá se pro správu BTS, 3.vrstva[3]

2.3.3 IS-95

I přestože jako technologie druhé generace značně dominuje GSM, vyskytly se zde některé jiné technologie, které se snažily využít jiného přístupu k médiu než jako právě zmíněné GSM, které využívá technologii přístupu TDMA. Asi jednou z nejznámější "alternativní" technologií je IS-95, která k přístupu k médiu využívá technologii CDMA. Hlavním důvodem pro použití CDMA namísto TDMA je hlavně počet účastníků, který je možné obsloužit. Tento počet je ve srovnání s TDMA až desetinásobný. IS-95 se oproti GSM liší také strukturou, pomocí které je provozována komunikace mezi základnovou stanicí a mobilní stanicí. Dopředné spojení od základnové stanice k mobilnímu zařízení se skládá z 64 logických CDMA kanálů, kde každý obsazuje stejnou 1228 kHz šířku pásma[3].

Podle využití jednotlivých kanálů je možné je rozdělit na:

- Pilotní kanál (kanál 0) - využívá se pro porovnávání síly signálů a rozhoduje o handoverech
- Paging kanály (kanály 1-7) -zajišťují zprávy pro mobilní stanice
- Traffic kanály (kanály 8-31 a 33-63) - určeny pro samotný uživatelský provoz v síti (rychlost původně 9.6 kbps, později navýšena na 14.4 kbps)
- Synchronizační kanál (kanál 32) - kanál vyhrazený pro určení buňkového systému (systémový čas, protokoly...)

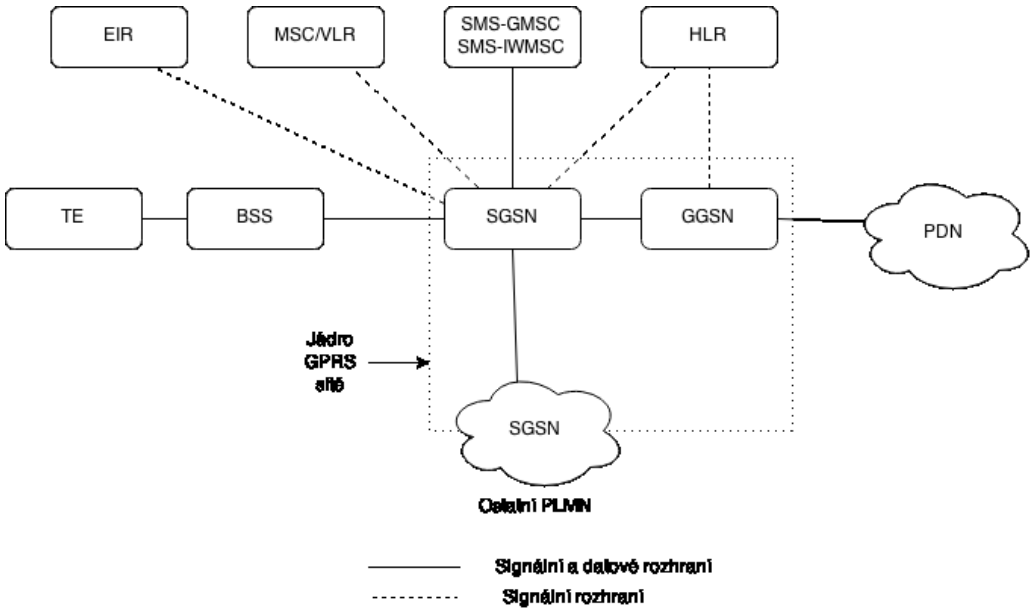
Všechny tyto kanály využívají stejné frekvenční pásmo a pro rozlišení jednotlivých uživatelů je použit 64-bitový chipping code. Zpětné spojení se skládá z 94 logických CDMA kanálů využívajících opět 1228 kHz šířku pásma a podporuje až 32 přístupových kanálů a až 62 kanálů pro uživatelský provoz. Protože jsou zpětné kanály využity ve směru od mobilní stanice k základnové stanici, využívají se k sestavení hovorů a nalezení současné pozice během handoverů. Dále jsou uvedeny některé z významných rozdílů mezi TDMA a CDMA.[3]

- Kapacita sítě - využití stejné frekvence je oproti TDMA možné i v sousedních buňkách z důvodu odlišení jednotlivých účastníků kódem. Díky tomu je kapacita této sítě až desetkrát větší než u TDMA
- Zabezpečení - protože technologie CDMA využívá rozprostřeného spektra, jsou signály zakódovány náhodně a není tudíž možné jej dekódovat, pokud neznáme náhodný kód pomoci kterého je zakódován
- Soft Handovery - CDMA může využívat tzv. soft handoverů, kdy je stanice zároveň registrována v obou buňkách, dokud není handover dokončen. Toto je sice zajímavějším řešením jak zvládat handovery oproti TDMA hard handoverům ale také značně složitějším

- CDMA je oproti TDMA novější a ne tak zcela probádanou technologií, která se ale stále rychle vyvíjí

2.3.4 GRPS (2.5G)

GPRS označuje nástavbu pro sítě druhé generace, kdy je využito přepojování paketů a je tak dosaženo vyšších přenosových rychlostí při posílání a stahování dat. Teoreticky tato technologie nabízí rychlost až 160 Kbps ovšem skutečná rychlost je poněkud menší, zhruba 56 Kbps pro stahování a 14.4 Kbps pro upload. GPRS využívá stejné rádiové kanály jako standardní GSM a nevyžaduje tedy nové frekvenční spektrum. Dá se tedy říct, že GRPS překrývá původní GSM které využívá přepojování okruhů a tímto je zajištěná možnost využít paketově orientovaného přenosu dat. Architektura sítě GPRS je uvedena a popsána na obrázku níže.[3]



Obrázek 2.5: *Architektura sítě GPRS*

- Gateway GPRS support node (GGSN) - zprostředkovává spojení s externími paketovými sítěmi (PDN). Směruje také pakety do SGSN a zpět do PDN. Příkladem PDN je například internet.
- Serving GPRS support node (SGSN) - stará se o doručování do a z mobilní stanice v určené oblasti, routing a samotný přenos a účtování služby.
- Ostatní prvky plní stejnou funkci jako u GSM (EIR, HLR, MSC...)

2.3.5 EDGE (2.75G)

Poslední technologií, která je považována za mezikrok mezi druhou a třetí generací, je Enhanced Data Rates for GSM Evolution (EDGE). Opět se jedná o využití v oblasti datových přenosů, tentokrát za použití nového druhu modulace a to konkrétně 8-PSK, která umožňuje přenos tří informačních bitů za použití jednoho symbolu na rádiové vrstvě. U technologií GSM nebo GPRS to

byl pouze jeden bit na jeden symbol. Teoreticky je možné u EDGE dosáhnout rychlosti až 500 Kbps, v praxi jsou pak běžné rychlosti poloviční. Protože je EDGE rozšířením služby GPRS, využívá stejnou architekturu, rozdíl je však v použité modulaci.[3]

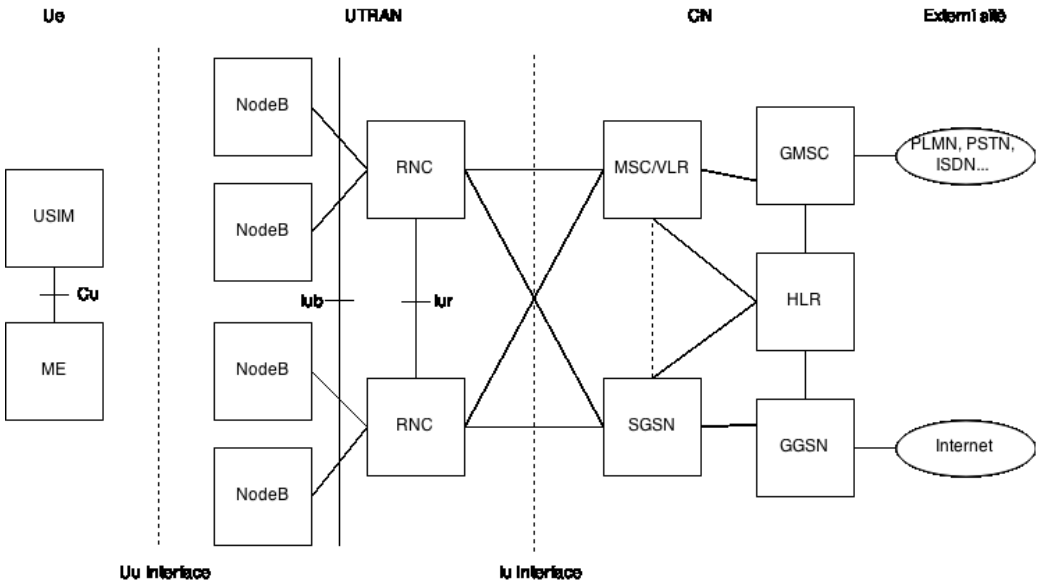
2.4 Sítě 3. generace (3G-3.9G)

3G je označení pro sadu standardů pro mobilní telekomunikační služby, které splňují specifikace IMT-2000 určené ITU. Tato iniciativa zahrnuje celou rodinu 3G standardů, jakými jsou UMTS, CDMA2000 nebo Mobile WiMAX. 3G nabízí velice rychlý přenos dat a jeho využití lze nalézt například v možnosti videohovorů, sledování mobilních přenosů televizních vysílání nebo přístupu na internet. Jedním z cílů 3G je také sjednocení standardů a využitých technologií pro výstavbu telekomunikačních sítí.[6]

2.4.1 UMTS (Universal Mobile Telecommunications System)

Za touto zkratkou se skrývá 3G systém, který vznikl v Evropě a dnes je využíván po celém světě. Hlavní myšlenkou tohoto systému je využití stejné technologie kdekoliv na světě, tak aby byl uživatel schopný používat stejné služby, které je zvyklý používat, nezávisle na místě na kterém se nachází nebo na použitém přístupu (satelitní, pozemní). UMTS využívá jak TDMA v již zavedených GSM pásmech, tak nově W-CDMA v pásmu 1.9–2.2 GHz. Rychlosti přenosu se zde pohybují od 384 kbps v základním UMTS přes 14Mbps u HSDPA až po 84.4 Mbps u HSDPA+. Architektura sítě se opět od minulých dvou generací liší.[6]

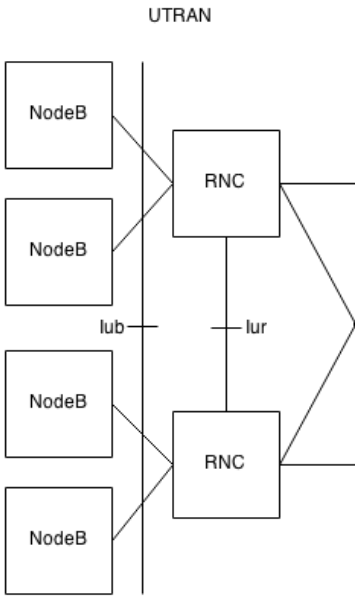
- NodeB - označení základnové stanice v systému UMTS, obsahuje antény, kabeláž, zdroj a je také schopná měřit kvalitu přijímaného signálu (RxLev, Ec/Io)
- Radio Network Controller (RNC) - spravuje a řídí NodeB a rádiové zdroje (RRC - radio resource control), také se stará o zabezpečení a QoS
- Gateway MSC (GMSC) - ústředna pro okruhově přepínané služby
- Serving GPRS Support Node (SGSN) - přepojování paketově přepínaných služeb
- Gateway GPRS Support Node (GGSN) - stejný význam jako u GPRS - zprostředkovává spojení s externími paketovými sítěmi (PDN)[6]



Obrázek 2.6: *Architektura sítě UMTS[7]*

Samotná síť UTRAN (stojící vedle standardní GSM přístupové sítě, označované jako GERAN), která využívá W-CDMA a pracuje na kmitočtech 1900–2200 MHz se skládá z následujících částí:

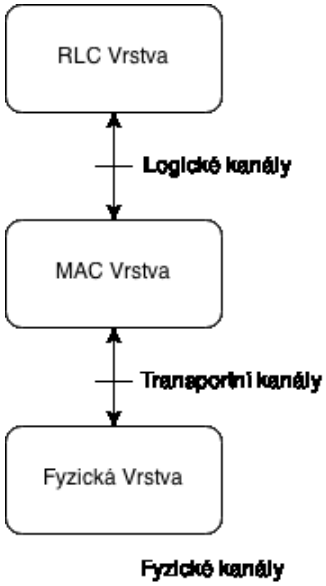
- Jeden nebo více Radio Network Subsystem (RNS), který je subjednotkou UTRAN a obsahuje jeden Radio Network Controller (RNC) a jednu nebo více NodeB
- Rozhraní Iub pomoci kterých jsou propojeny jednotlivé RNC
- Rozhraní Iub pomoci kterých jsou propojeny RNC a NodeB[6]



Obrázek 2.7: *Architektura přístupové sítě UTRAN[7]*

V přístupové síti UTRAN se dále vyskytují tři různé druhy kanálů (Fyzické, transportní a logické). Tyto kanály se vyskytují mezi třemi nejnižšími vrstvami (Fyzická, MAC a RLC). Nejdříve tedy stručný popis samotných vrstev a k čemu slouží:

- Fyzická vrstva - zde dochází ke kódování transportních kanálů do CCTrCH (Coded Composite Transport Channel), což je datový proud, který vzniká právě kódováním a multiplexováním jednoho nebo více transportních kanálů.
- MAC vrstva - zajišťuje řízení přístupu do fyzického rádiového kanálu
- RLC vrstva - stará se o segmentaci, sestavování a spojovaní dat, dále pak také o kontrolu chyb které mohly vzniknout při přenosu, šifrování a přenos uživatelských dat. Tato vrstva je potřebná při přenosu většího objemu dat, kdy vznikají také častěji chyby při přenosu.[6]



Obrázek 2.8: *Rozložení kanálů a vrstev v UMTS[9]*

Co se samotných kanálů mezi těmito vrstvami týče, existují tři – logické, transportní a fyzické, přičemž každé z těchto kanálů můžeme ještě rozdělit na podkategorie. Logické kanály, které definují typ dat, který bude přenášen, můžeme rozdělit na řídící a provozní. Transportní kanály nám pak určují jakým způsobem a s jakými vlastnostmi jsou data přenesena pomocí fyzické vrstvy, tyto můžeme rozdělit na společné a vyhrazené. Posledními kanály jsou kanály fyzické, které charakterizují samotný rádiový kanál, tyto kanály lze rozdělit na ty, které se používají pro downlink a ty, které jsou využity pro uplink. [6]

Logické kanály

- **Řídící**
  - **BCCH (Broadcast Control Channel) -** přenáší řídící informace o buňce

- **PCCH (Paging Control Channel) -** slouží k přenosu informací o příchozích žádostech o spojení
- **DCCH (Dedicated Control Channel) -** slouží pro obousměrný přenos informací k UE
- **CCCH (Common Control Channel)** - slouží k přenosu řídící informace mezi sítí a uživateli[7,9]

- **Provozní**
  - **DTCH (Dedicated Traffic Channel) -** přenos informací jednomu uživateli
  - **CTCH (Common traffic Channel) -** přenos informací pro skupinu uživatelů[7,9]

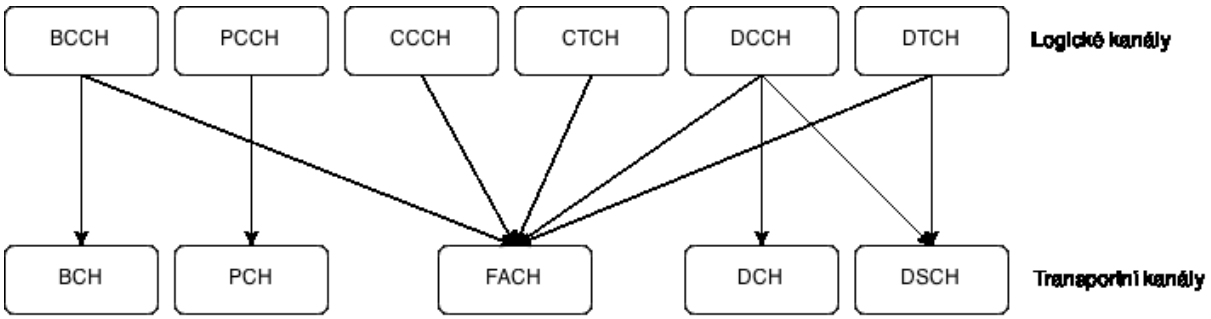
Transportní kanály

- **Vyhrazené**
  - **DCH (Dedicated Channel) -** obousměrný kanál, který se používá pro přenos řídících informací i pro přenos uživatelských dat
- **Společné**
  - **BCH (Broadcast Channel) -** informuje o specifikacích systému a buňky, využívá maximální výkon pro dosažení všech uživatelů v buňce
  - **PCH (Paging Channel) -** pro přenos stránkovacích a oznamovacích zpráv (navazání spojení s uživatelem...)
  - **FACH (Forward Access Channel) -** přenáší řídící informace uvnitř buňky, také může přenášet malé množství dat (cca. kB)
  - **RACH (Random Access Channel) -** uplink kanál, přenáší informace od uživatel k síti (sestavení spojení, registrace do sítě...)
  - **CPCH (Common Packet Channel) -** slouží pro přenos malého množství dat
  - **DSCH (Downlink Shared Channel) -** downlink kanál využívaný pro více UE, možnost změny rychlosti při každém jednotlivém rámci[7,9]

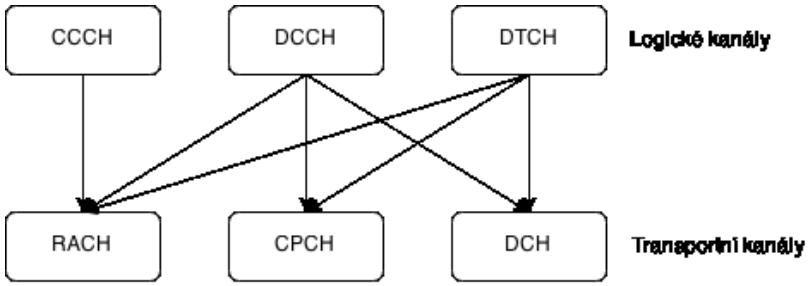
Fyzické kanály

- **Uplink**
  - **DPDCH (Dedicated Physical Data Channel) -** datový přenos
  - **DPCCH (Dedicated Physical Control Channel) -** přenos řídících informací
  - **PRACH (Physical Random Access Channel) -** přenáší RACH
  - **PCPCH (Physical Common Packet Channel) -** přenáší CPCH
- **Downlink**
  - **PCCPCH (Primary Common Control Physical Channel) -** přenáší BCH
  - **SCCPCH (Secondary Common Physical Channel) -** přenáší FACH a PCH
  - **PDSCH (Physical Downlink Shared Channel) -** přenáší DSCH
  - **CPICH (Common Pilot Channel)** - určený pro synchronizaci a identifikaci scramblovacího kódu základnové stanice[7,9]

Na následujících obrázcích je zobrazeno mapování jednotlivých logických kanálů do transportních, schémata jsou rozdělena podle směru, ve kterých jsou využívány.



Obrázek 2.9: *Mapování logických kanálů do transportních - směr downlink[9]*

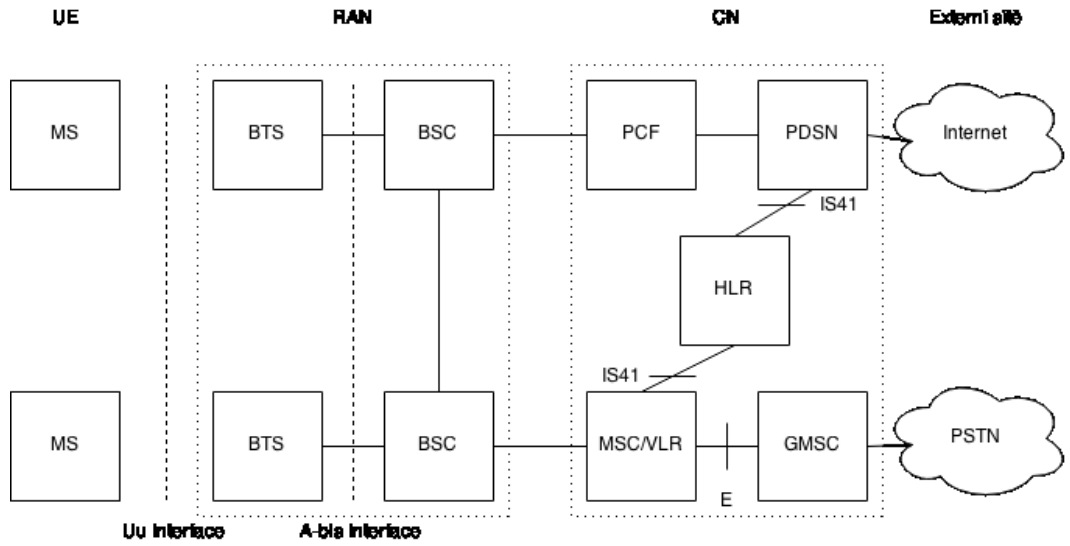


Obrázek 2.10: *Mapování logických kanálů do transportních - směr uplink[9]*

2.4.2 CDMA2000

CDMA2000 je označení rodiny standardů pro mobilní sítě sloužící pro komunikaci mobilních telefonů se sítí využívající kódový multiplex (odtud název CDMA). CDMA2000 je založena na technologii druhé generace – IS-95, je jejím přímým pokračovatelem a je s touto technologií také zpětně kompatibilní díky tzv. Multi-Carrier konfiguraci, kdy je dostupná šířka pásma rozdělená do několika nosných vln. Uživatelská data jsou pak demultiplexována a rozprostřena do několika oddělených kanálů.

Technologie CDMA2000 je používána především v zemích Východní Asie a Severní Ameriky, ale je možné se s ní setkat i u nás, protože se zde využívá pro přenos datových služeb. Svojí rozšířeností tedy zaujímá na příčce technologií třetí generace druhé místo ihned za UMTS.[6]



Obrázek 2.11: *Architektura sítě CDMA2000[6]*

Architektura sítě CDMA2000 je v základních stavebních prvcích podobná síti UMTS, je zde však odlišnost, kdy má BSC již zabudovanou funkci Packet Control Function (PCF) sloužící ke kontrole dostupných rádiových zdrojů a k zajištění stálého spojení při komunikaci mezi mobilním zařízením a externí sítí. PCF také může sloužit k bufferování dat, která jsou posílána z PSDN dokud nebude volný příslušný komunikační kanál.[6,8]

Technologie samotná prošla od svého uvedení několik vývojovými změnami, hlavně z hlediska rychlosti přenosu a s tím spojené rozšiřování šířky kanálu. První variantou byla CDMA2000 1xRRT (Radio Transmission Technology), která využívala stejné rádiové pásmo a šířku kanálu jako předchůdce IS-95 ovšem s tím rozdílem, že bylo přidáno dalších 64 ortogonálních kanálů ke stávajícím 64. Tímto bylo dosaženo téměř zdvojnásobení kapacity od původního IS-95. Rychlost přenosu paketových dat se zde pohybuje až do teoretického maxima 152 kbps, přičemž reálná rychlost se pohybuje v průměru okolo 80 kbps. [6,8]

Dalším vývojovým stupněm je pak CDMA2000 1xEV-DO poskytující lepší přenosové rychlosti. Je zde využito jak samotného CDMA přístupu tak i TDMA k dosažení maximální přenosové rychlosti.[8]
Podle jednotlivých revizí tohoto standardu se pak liší jednotlivé přenosové rychlosti, kdy pro revizi 0 je rychlost ve směru downlink 2,4 Mbps pro uplink pak 153 kbps. Revize A pak nabízí až 3,1 Mbps v downlink směru a 1,8 Mbps ve směru opačném, v této revizi se také poprvé objevila podpora pro QoS a VoIP. Poslední vývojový stupeň, revize B, nabízí rychlosti až 14.7/5.4 Mbps. Následníkem těchto standardů se měla stát revize C, také označována jako Ultra Mobile Broadband (UMB), ale vzhledem k pokusu technologie LTE o sjednocení existujících standardů, od ní bylo upuštěno.[8]

Tabulka.2.1: Přehled přenosových rychlostí CDMA2000[8]

Označení	Rychlost downlink	Rychlost uplink	Šířka kanálu
CDMA2000 1xRRT	2,4 Mbps	153 kbps	1,25 MHz FDD
CDMA2000 1xEV-DO rev. 0	2,4 Mbps	1,8 Mbps	1,25 MHz FDD
CDMA2000 1xEV-DO rev. A	3,1 Mbps	1,8 Mbps	1,25 MHz FDD
CDMA2000 1xEV-DO rev. B	14,7 Mbps	5,4 Mbps	5 MHz FDD

2.4.3 HSPA, HSPA+ (3.75G)

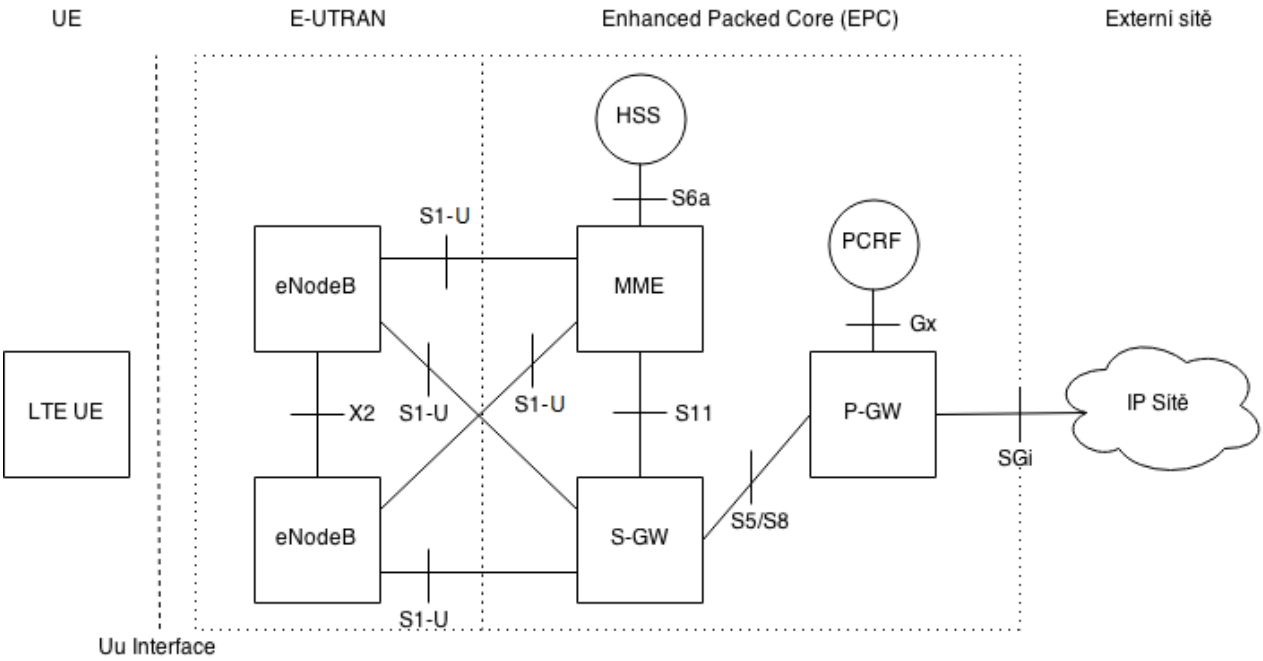
Obecná charakteristika a důvod, proč označovat další revize, releasy a ostatní věci souvisící s nárůstem rychlosti v dané generaci mobilní sítě, je jednoduchá – jde hlavně o záměr operátorů ukázat, že nabízejí "ještě něco navíc, než předtím". Tím se většinou myslí právě zrychlení přenosu dat ať už od uživatele nebo k němu. Stejně jako v případě GPRS a EDGE v sítích druhé generace, i zde, v technologii UMTS bylo dosaženo pokroku, který umožňuje nárůst v rychlosti přenosu. Jako první se objevila technologie HSDPA v UMTS Release 5. Tato technologie zvýšila rychlost přenosu směrem k uživateli, v ideálním případě, z původních 384 kbps na 14,4 Mbps díky použití modulace 16QAM , zrušení Fast Power Control, snížení času TTI (Transmission Time Interval) z 10 ms na 2 ms a zavedení techniky H-ARQ. V Release 6, pak byla definována úprava, která upravila rychlost ve směru uplink – tzv. HSUPA, která se snažila adoptovat vylepšení, která byla použita pro HSDPA a použit je pro přenos ve směru od uživatele. Byl tak zaveden nový kanál Enhanced Dedicated Channel (E-DCH), který není sdílený jako HS-DSCH, doba TTI se stejně jako u HSDPA snížila na 2 ms a byla použita technika Fast Packet Scheduling. Ideální rychlost pro HSUPA se pak pohybuje okolo 5,76 Mbps. Souhrně jsou tyto dvě technologie nazývány jako HSPA a označeny za 3.75 generaci.[13]

Dalším vývojovým stupněm je tzv. HSPA+, které bylo představeno v Release 7 a které díky zavedení 64QAM modulace pro downlink, 16QAM pro uplink a agregaci více nosných, dovoluje teoretické rychlosti přenosu až 56 Mbps pro downlink a 22 Mbps pro uplink, samozřejmě, toto jsou rychlosti na buňku, takže těchto rychlostí asi těžko uživatel dosáhne. HSPA+ bývá označována jako 3.9G, stejně jako LTE.[13]

2.4.4 LTE (3.9G)

LTE, narozdíl od LTE-Advanced, je standardem stále spadajícím do 3G, někteří operátoři jej ale i přesto, že nesplňuje kritéria technických požadavků definována v IMT-Advanced, uvádí nesprávně jako 4G. LTE bylo definováno v Release 8, s drobnými dodatky a úpravami v Release 9. Samotné LTE by mělo být teoreticky schopné nabídnout rychlosti až 300 Mbps pro stahování a 75 Mbps pro upload a využívá pouze technologii přepojování paketů (na rozdíl od hovorů v

UMTS/CDMA2000, které probíhá pomocí přepínaní okruhů). Disponuje také lepšími přenosovými rychlostmi pro rychle se pohybující mobilní zařízení, nabízí podporu pro streamovaný obsah a také zaznamenává zlepšení v odezvě při nízkých datových přenosech, které se pohybují v ideálních podmínkách pod 5 ms. Pro přenos ve směru k uživateli je použito OFDMA, pro přenos od uživatele pak SC-FDMA kvůli úspoře energie. Frekvenční pásmo je pak tvořeno ze všech dostupných frekvencí, které jsou používány v 3G (v Severní Americe pásma 700, 750, 800, 850, 1900, 1700/2100, 2500 a 2600, v Evropě pak pásma 700, 800, 900, 1800, 2600). Co se týká velikosti buněk, je možné LTE provozovat od buněk, které mají poloměr několik desítek metrů (pikobuňky) až po obrovské makrobuňky o poloměru 100 km.[12,13]



Obrázek 2.12: *Architektura LTE[13]*

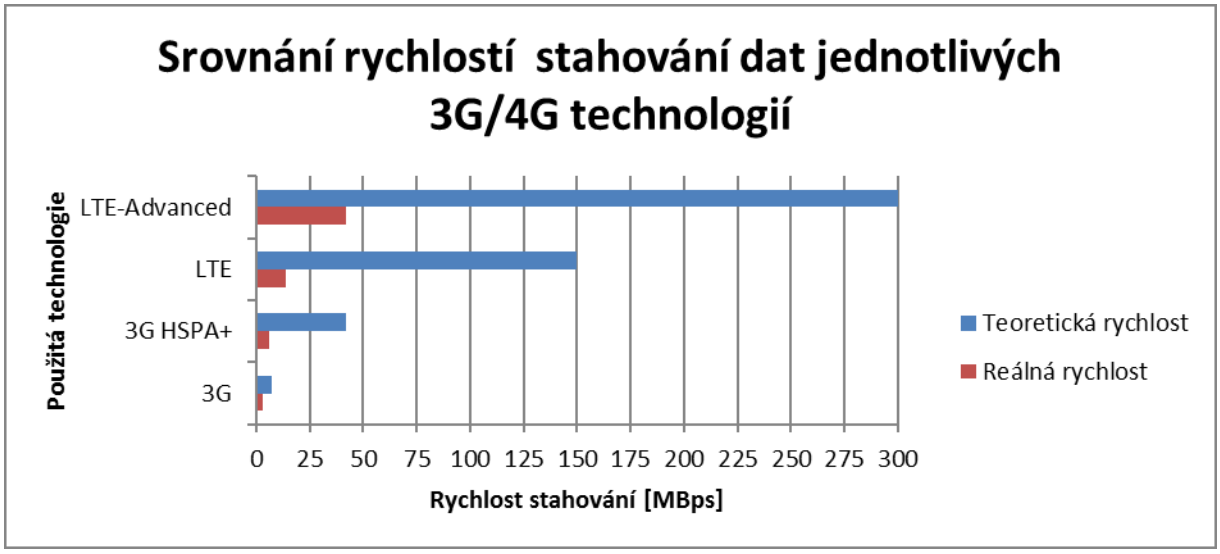
- Evolved NodeB (eNodeB) - základnová stanice v síti LTE, stará se o přenos paketových dat, kontrolu mobility nebo vytížení kanálů. EnodeB jsou mezi sebou propojeny pomoci rozhraní X2 (logické spojení)
- Mobility Management Entity (MME) - zastřešuje služby spojené se zpracováním signalizace a NAS zpráv, které obsahují autorizační informace, sestavení a udržování IP konektivity mezi UE a PGW
- Serving Gateway (SGW) - směruje a zpracovává datové pakety od EnodeB přes rozhraní S1-U
- PDN Gateway (PGW) - stará se o konektivitu k PDN (Například do Internetu)
- Home Subscriber Server (HSS) - uchovává informace uživatelích a provádí jejich autentizaci a autorizaci, poskytuje také informace ohledně účastníkovy polohy a jeho IP adresy.
- User Equipment (UE) - Telekomunikační koncové zařízení uživatele[13]

Pro zřízení LTE sítě pro výzkumné účely je možné použít open-source software OpenLTE, který z rádiové periférie (např. B210 od společnosti Ettus), dokáže vytvořit přístupový bod eNodeB. Vytvoření takovéhoto eNodeB a otestování jeho vlastností (přenosová rychlost, stabilita, možnosti které nabízí) je právě cílem této diplomové práce.

2.5 Sítě 4. generace (4G)

Sítě čtvrté generace znamenají opět nárůst v rychlosti datových přenosů, podle požadavků IMT Advanced definované ITU by měla teoretická rychlost přenosu dosahovat až 1 Gbps/500 Mbps. Hlavní technologií by se měla stát LTE-Advanced, která vychází z LTE, využívá stejnou architekturu sítě a je s ní také zpětně kompatibilní. V době psaní této diplomové práce je LTE-Advanced dostupná jen v několika málo městech České republiky, konkrétně na Pelhřimovsku, na Vysočině a v Praze (O2), dále pak v Mladé Boleslavi (T-Mobile) a v Karlových Varech (Vodafone). LTE-Advance využívá technologii Carrier Aggregation, kdy dochází ke spojování několika frekvenčních pásem, v České republice je to spojení dvou pásem – 800 a 1800 MHz. Dále je pak využitá metoda MIMO pro dosažení větší rychlosti za použití více vysílacích a přijímacích antén zároveň. V současné době je maximální teoretická rychlost přijímání dat pomoci LTE-Advanced zhruba 300 Mbps, odesíláni pak až 50 Mbps. Tyto hodnoty jsou však vztaženy na buňku a pro jediného registrovaného účastníka v ní, ve skutečnosti se naměřená rychlost pro stahování pohybuje okolo 50 Mbps.

V současné době také není používáno velké množství mobilních zařízení, které by podporovaly LTE-Advanced, zátěž tedy zatím není tak velká a hodnoty se budou během několika měsíců a let podstatně měnit, ať už příznivě díky vývoji technologie nebo negativně kvůli nárůstu uživatelů kteří budou LTE-Advanced využívat.



Obrázek 2.13: *Přehled rychlostí pro jednotlivé technologie*

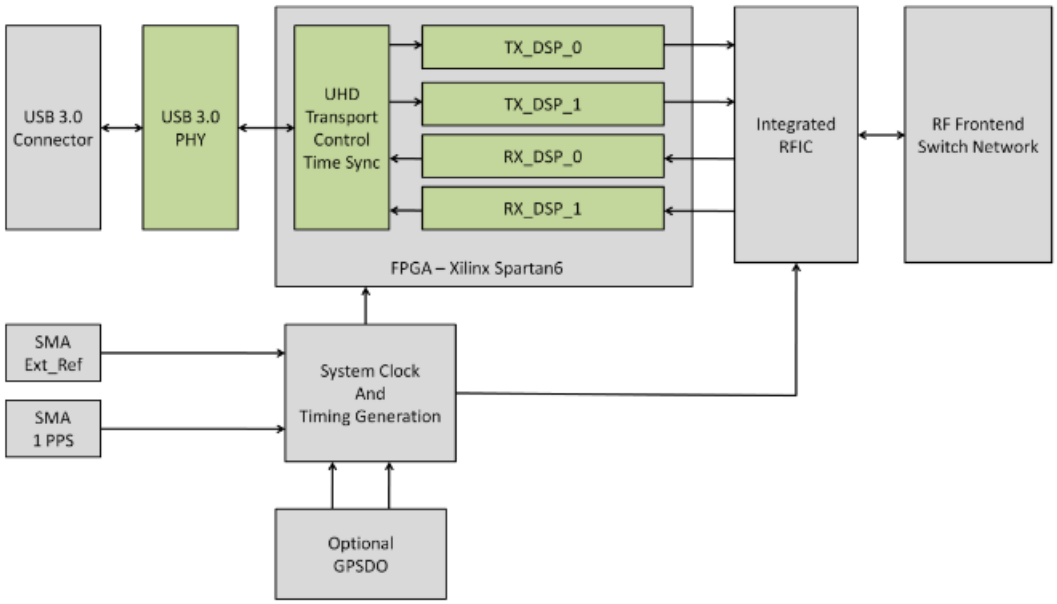
3 Vlastnosti a využití USRP

USRP je označení pro rodinu softwarově řízených rádiových periferií od společnosti Ettus Research. Pro softwarová rádia obecně platí, že je funkcionalita některých hardwarových komponent rádia, zprostředkována jejich softwarovou implementací pro osobní počítače. USRP je vytvořeno především k testování a výzkumu široké škály možností rádiových sítí, taktéž je možné tento hardware využít pro amatérské účely, díky poměrně dostupné ceně, ovšem častěji je možné se s tímto hardwarem setkat právě ve výzkumných ústavech, školách a podobně. USRP je k počítači připojeno pomoci vysokorychlostního připojení, dnes už se u většiny modelů využívá připojení s hostitelskou stanicí přes USB 3.0. U některých modelů se také vyskytuje omezená stand-alone funkcionalita, kdy je hardware schopen fungovat a nabízet některé ze svých funkcí i bez podpory hostitelského počítače. Pro většinu USRP je ovšem potřeba připojit jej k hostitelskému počítači, který obsahuje požadovaný software a určuje nám, jak bude USRP využito. K tomu, aby mohla USRP s počítačem komunikovat je zapotřebí takzvaných USRP hardware driver (UHD) ovladačů, které nám zajistí právě propojení softwarové části softwarového rádia z hostitelského počítače s hardwarem základní desky USRP. Tyto ovladače, stejně jako software, kterým definujeme funkcionalitu USRP, jsou z velké části open-source a je možné je tedy nejen zdarma využívat, ale v případě zájmu se zapojit do jeho vývoje.[10]

Obrázek 3.1: *Základní deska USRP B210[11]*

V této diplomové práci je využito pro tvorbu OpenLTE přístupového bodu USRP řady B210, od starší B100 se liší především podporou USB 3.0 rozhraní a podporou 2x2 MIMO, také už není potřeba mít samostatný napájecí kabel, ale napájení je nyní zprostředkováno právě pomoci USB kabelu. Toto USRP je schopné pracovat na frekvenčním rozsahu 70 MHz – 6 GHz.[11]

Na základní desce se nachází programovatelné hradlové pole Xilinx Spartan 6 XC6SLX150, rozhraní USB 3.0 a konektor pro napájení ze sítě, integrovaný RFIC okruh schopný pracovat na frekvencích 70 MHz – 6 GHz, dále pak dva konektory pro přijímací anténu a dva pro vysílací. Nakonec zde nalezneme konektory pro připojení GPSDO modulu a PPS pro synchronizaci hodinového signálu. Deska USRP je modulární a tak je možné využít různých dalších zásuvných modulů – tzv. "daughterboard" pro rozšíření funkcí. Také je možné využít různých druhů antén, které je možné připojit pomoci SMA-SMA kabelu, nebo přímo zašroubovat do příslušného konektoru.[10,11]



Obrázek 3.2: *Blokové schéma USRP B210[11]*

USRP je možné využít opravdu k velkému množství funkcí, jednou z nich je právě ta, kterou se zabývám v této diplomové práci a to vytvoření přístupového bodu LTE sítě pomoci open-source softwaru OpenLTE. Mezi další možnosti využití USRP patří:

- Čtečka RFID určená pro zpracování identifikace na rádiové frekvenci, RFID čipy jsou dnes velmi často používány k identifikaci zboží v obchodech nebo pro aktivní lokalizaci. S využitím tohoto softwaru je možné číst údaje uložené v RFID čipu.

- Využití jako pasivní radar, kdy je možné zachytávat rádiové signály vyslané např. letadly a pomoci těchto signálů je možné určit do omezené vzdálenosti polohu. Také je možné získávat informace z meteorologických radarů a podobně.
- Přijímač WiMAX signálu, dostupné ovšem pouze pro USRP řady N2xx.
- USRP lze také použít jako FM rádio vysílač i přijímač.
- Přijímač GPS signálu.
- Zařízení pro testování chybovosti v rádiových sítích.
- V neposlední řadě lze USRP využít i pro tvorbu přístupového bodu v klasické GSM síti, kdy je USRP schopné, například s využitím pobočkové ústředny Asterisk, jako plně funkční základnová stanice schopná zpracovávat hovory, SMS i dodatkové služby jako je schránka nebo IVR služba.
- Skenování frekvenčního pásma
- Zachytávání 802.11a/g/p komunikace

USRP řady N210 a USRP2 jsou plně kompatibilní s programy MATLAB a Simulink, je možné tedy využít tyto programy pro tvorbu grafů nebo podrobnějšímu zpracování a analýze informací.

4 Návrh a realizace eNodeB prvku s využitím USRP

V této části se budu již prakticky zabývat postupem, jakým je možné vytvořit vlastní LTE přístupový bod eNodeB s využitím softwarově definovaného rádia USRP B210 od společnosti Ettus a open-source projektu OpenLTE. Je potřeba vzít na vědomí, že je tato práce psaná v prvním čtvrtletí roku 2015 a je tak možné, že některé postupy/software již nemusí být aktuální a některé aplikace mohou být nahrazeny jinými.

4.1 Instalace a konfigurace softwaru

Pro vytvoření experimentálního prostředí pro realizaci OpenLTE přístupového bodu je potřeba využít následující hardware a software:

- PC s USB 3.0 portem
- Operační systém na bázi Linuxu
- USRP B210
- GNU Radio
- Mobilní zařízení podporující LTE
- OpenLTE software
- SIM Programátor s prázdnou USIM Kartou využívající MILENAGE algoritmus a patřičný software pro programování sim karet nebo jakákoliv USIM karta s MILENAGE algoritmem, ke které je ovšem nutné znát Ki klíč a IMSI

4.1.1 Linux Mint 17.1

Jako operační systém jsem zvolil Linux Mint 17.1 s grafickým rozhraním Cinnamon. Je prakticky jedno, jaká linuxová distribuce bude použita, ovšem z důvodu co nejaktuálnějšího pracovního prostředí, jsem zvolil právě operační systém vycházející z Ubuntu 14.04 LTS. Mint byl zvolen jen z důvodu příjemného pracovního prostředí. OpenLTE nelze provozovat ve virtuálním prostředí, ať už z důvodu omezených systémových prostředků, nebo kvůli možným problémům se síťovým rozhraním. Lze ovšem použít (avšak výrazně nedoporučuji) některé z LiveCD distribucí, například specializovanou distribuci GNURadioLiveDVD, kterou spravují lidé z projektu GNURadio. I zde ovšem platí, že rychlost u přenosu dat mezi PC a USRP je s takovou distribucí výrazně zpomalená a distribuce nemusí obsahovat aktuální software. Zvolený Linux Mint byl tedy nainstalován jako druhý systém vedle Windows 7 x64.

4.1.2 GNU Radio, UHD driver a prerekvizity

Základním prvkem pro využití jakéhokoliv softwarově definovaného rádia je software GNU Radio a také ovladače pro komunikaci mezi USRP a PC, takzvané UHD neboli USRP Hardware driver. Všechny tyto ovládací prvky a jejich závislosti v aktuální verzi je možné stáhnout pomoci

vytvořeného skriptu ze stránek www.sbrac.org. Konkrétně je možné postupovat následujícími příkazy, zadanými přímo do terminálu operačního systému:

```
mkdir gnuradio
cd gnurdio
wget http://www.sbrac.org/files/build-gnuradio
chmod a+x build-gnuradio
```

V tomto skriptu je pak nutné ještě upravit všechny výskyty výrazu `"libzmq"` na `"libzmq1"` z důvodu jiného názvu balíčku. Poté již stačí spustit skript příkazem

```
./build-gnuradio -v
```

Celá operace (stahování, kompilace, instalace) může v závislosti na výkonu počítače trvat až tři hodiny. Po dokončení instalace by již měly být nainstalovány všechny důležité součásti pro spuštění USRP. Správnost je možné ověřit připojením USRP B210 a zadáním příkazu `uhd_usrp_probe` nebo `uhd_find_devices`. Pokud se zobrazí údaje o připojeném USRP a jeho parametrech, je vše v pořádku a můžeme přistoupit k samotné instalaci OpenLTE.

4.1.3 OpenLTE

OpenLTE má své vlastní projektové stránky na adrese http://sourceforge.net/projects/openlte/, zde je možné stáhnout nejnovější verzi, nebo je možné využít git pro stažení přímo z repozitáře:

```
git clone git://git.code.sf.net/p/openlte/code openlte-code
```

Po stažení aktuální verze je nutné archív rozbalit, přepnout se do složky s rozbalenými soubory a OpenLTE zkompilovat a nainstalovat následujícími příkazy:

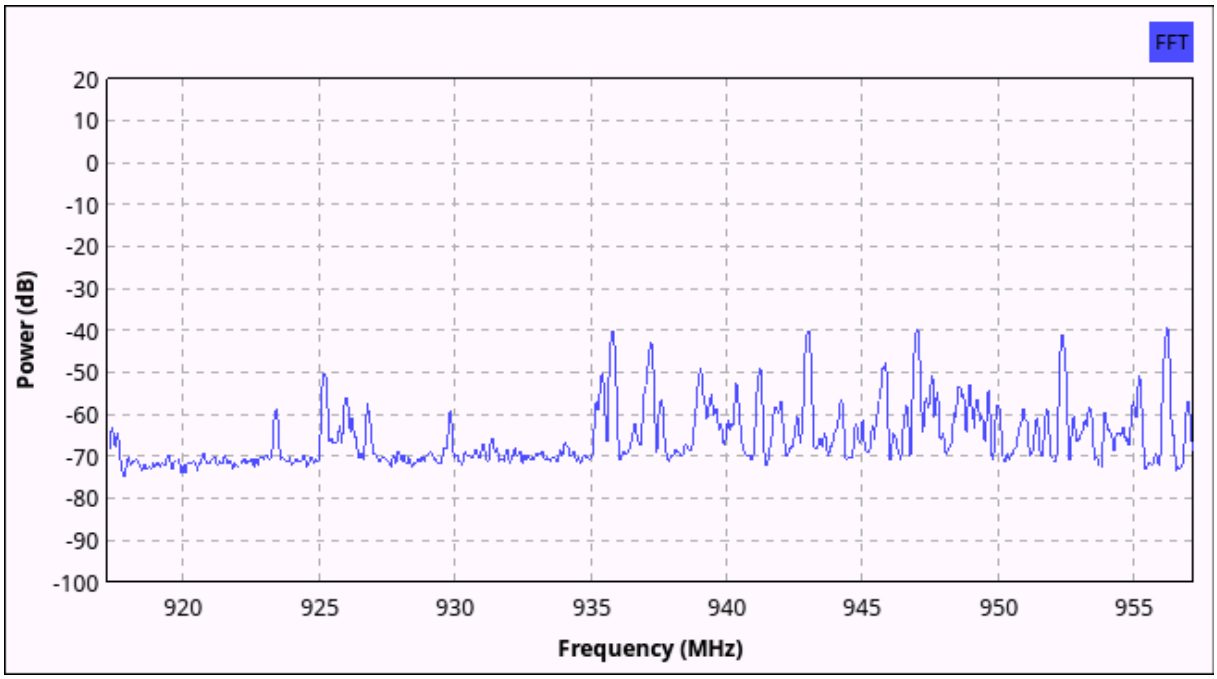
```
mkdir build
cd build
sudo cmake ../
sudo make
sudo make install
```

Poté je již možné začít využívat OpenLTE, je nutné také podotknout, že OpenLTE nenabízí jen možnost vytvoření vlastního přístupového bodu eNodeB, ale také nabízí jiné funkce, jako je například hledání LTE pásem v okolí, nebo přenos dat mezi dvěma USRP. Hlavní funkcionalitou je ovšem využití jako LTE eNodeB přístupový bod.

4.2 Realizace přístupového bodu LTE eNodeB

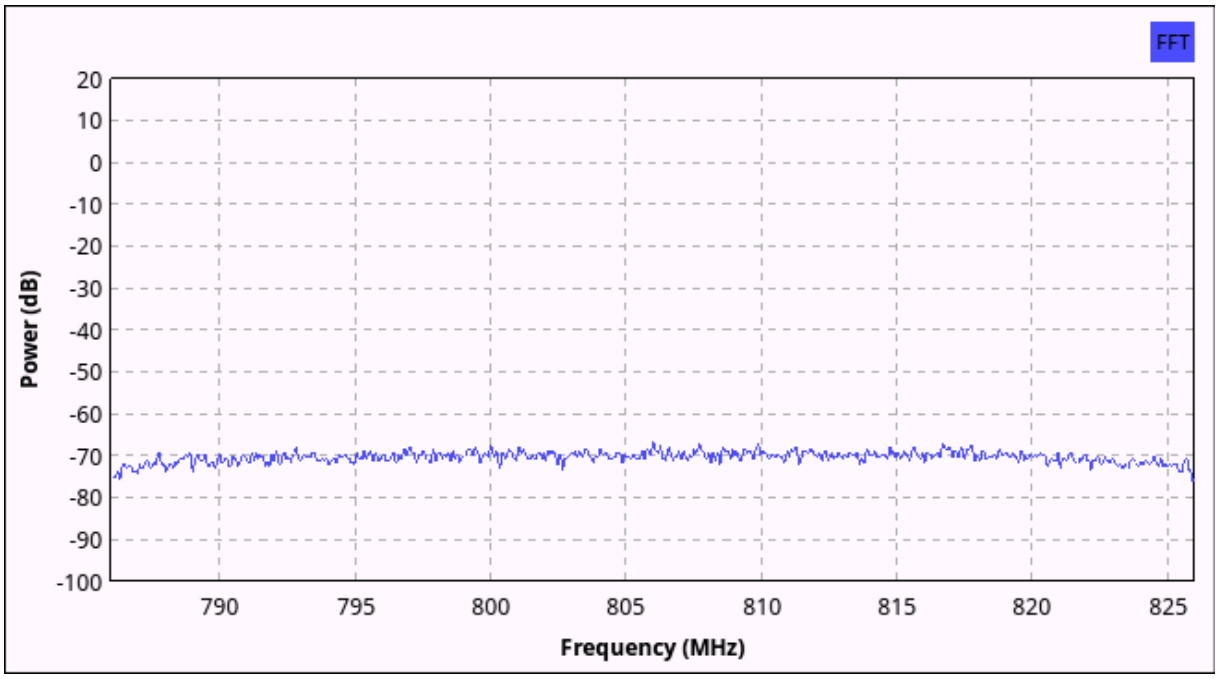
4.2.1 Spektrální analýza okolních pásem

Ještě před tím, než bude vytvořen a spuštěn přístupový bod, je nutné provést analýzu využití spektra mobilních sítí v okolí. Nejen že je tak možné docílit lepších výsledků při následném hledání přístupového bodu mobilním zařízením, ale také by se nikdy a za žádných okolností nemělo stát, že by někdo provozoval svou mobilní síť v již obsazeném frekvenčním pásmu. K tomuto je možné využít spektrální analyzér, nebo postačí i USRP B210, které funkci prozkoumání spektra také nabízí. Tuto funkci lze zapnout příkazem `uhd_fft` a následně můžeme zhodnotit, které pásmo lze využít. Protože v České republice jsou (nebo brzy budou) využívaná pásma pro LTE, které odpovídají UMTS pásmům 1, 3, 7, 8 a 20, je vhodné nejdříve podle jím přiřazených frekvencí prozkoumat tato pásma, neboť mobilní zařízení určené pro český trh také nemusí všechna pásma podporovat a nemuseli bychom být schopni se do OpenLTE sítě s nesprávnými parametry připojit. Na následujících obrázcích lze vidět rozdíl mezi obsazeným a volným pásmem. Analýza proběhla pomoci `uhd_fft` funkce.



Obrázek 4.1: *Analýza využití pásma GSM900 (Band 8)*

Zde je patrné využití frekvenčního pásma našimi standardními operátory (T-Mobile, O2, Vodafone), není tedy vhodné využívat toto pásmo pro experimentální OpenLTE síť.



Obrázek 4.2: *Analýza využití pásma 790-825 MHz (Band 20)*

Zde vidíme volné a zatím nevyužívané frekvenční spektrum Band 20. Na těchto frekvencích je tedy možné zřídit vlastní OpenLTE síť.

4.2.2 Vytvoření vlastní USIM karty

Pro to, aby se mohl účastník registrovat do OpenLTE sítě, je potřeba projít autentizačním procesem, podobně jako je tomu u standardních UMTS/LTE sítí. Proto je potřeba uložit parametry uživatele do databáze, vůči které se bude ověřovat jeho totožnost. Tyto parametry v OpenLTE tvoří trojice údajů:

- Autentizační Ki klíč
- Unikátní číslo SIM karty IMSI
- Unikátní číslo mobilního zařízení IMEI

Zatímco IMSI a IMEI čísla lze, ať už s menším či větším úsilím, získat, Ki klič je prakticky nezískatelný. Novější SIM karty obsahují nejen lepší šifrování tohoto klíče, ale také disponují bezpečnostním mechanismem, který v případě útoku brute force takovouto SIM kartu znehodnotí. Jedinou možností je tedy buď disponovat takovou USIM kartou, ke které IMSI i Ki známe, nebo si za pomoci programátoru a prázdné sim karty naprogramujeme vlastní USIM kartu, ke které tyto parametry zadáme a uschováme si je. Nutno podotknout, že použité prázdné sim karty musí být typu USIM a musí podporovat MILENAGE algoritmus, na kterém je postavena autentizační metoda COMP128-4 (využívající AES).

Pro programování testovacích USIM karet byly využity:

- Programátor BLUDRIVE II s podporou programování LTE/WDCMA USIM karet
- Testovací USIM karta s podporou MILENAGE algoritmu
- Aplikace PySIM

Nejdříve je nutné nainstalovat závislosti pomoci

```
sudo apt-get install pcscd pcsc-tools libccid
```

Dále je potřeba stáhnout Pyscard http://sourceforge.net/projects/pyscard/files/pyscard/ extrahovat, přepnout se do složky s extrahovanými soubory a spustit instalaci

```
sudo /usr/bin/python setup.py build_ext install
```

Nakonec nainstalujeme a spustíme aplikaci PySIM.

```
git clone git://git.osmocom.org/pysim pysim
cd pysim
./pySim-read.py
```

Při samotném programování je potřeba dávat pozor na zadávané údaje a ujistit se, že známe typ USIM karty. Ne všechny typy USIM karet jsou podporovány a jejich výčet lze nalézt na stránkách projektu PySIM. Dále je pak nutné postupovat opatrně po dokončení programování karty, protože i přesto, že si USIM programujeme sami, není možné zpětně zjistit Ki klíč z již naprogramované karty. Vzhledem k tomu, že Ki klíč spolu s IMSI je potřeba zadat do databáze uživatelů OpenLTE, je vhodné si poznačit tyto údaje ještě před samotným programováním.

Tímto příkazem provedeme samotný zápis na prázdnou USIM kartu, parametry označují typ použité karty a jednotlivé údaje USIM karty jako je právě Ki, IMSI, PIN, PUK MCC/MNC apod.

```
./pySim-prog.py -t sysmoUSIM -j 0 --op=63cdf50ee652415c1f45fa6537d
```

Po úspěšném dokončení je nám nabídnuta shrnující tabulka s naprogramovanými údaji

Insert card now (or CTRL-C to cancel)
Generated card parameters :
> Name : OpenLTEUSIM
> SMSP : e1ffffffffffffffffffff0581005155f5ffffffffffff000000
> ICCID : 8901901550000123456
> MCC/MNC : 001/01
> IMSI : 001010000123456
> Ki : 112233445566778899AABBCCDDEEFF
> OPC : 49cd0845dd1b0d819a496e27a16c0916
> ACC : None

4.2.3 Konfigurace OpenLTE

Nyní s vytvořenou USIM kartou, ke které známe Ki klíč a IMSI, je možné přidat účastníka do databáze OpenLTE. Nejprve je potřeba se připojit ke konzoli OpenLTE, otevřeme tedy tři terminálová okna a do první napíšeme `LTE_ffd_enodeb`. Objeví se hlavní okno OpenLTE, vyzývající k připojení k ovládací konzoli přes port 30000. Do druhého terminálu tedy napíšeme

```
telnet localhost 30000
```

Pro připojení se ke konzoli, která nám bude zprostředkovat logy a zobrazí signalizační komunikaci, použijeme port 30001, tedy `telnet localhost 30001`. Ovládací konzole na portu 30000 také nabízí možnost přímé konfigurace parametrů OpenLTE, po zadání příkazu `help` se zobrazí aktuální nastavení. Důležité parametry, které lze pro OpenLTE nastavit jsou:

- tx_gain - zisk vysílací antény
- rx_gain - zisk přijímací antény
- clock_source - zdroj hodinového signálu
- band - použité LTE pásmo
- bandwidth - šířka pásma v MHz
- debug_type - nastavení, jaké zprávy se budou v logu zobrazovat (error, info, debug, warning)
- n_ant - počet použitých antén, například pro MIMO přenos
- dl_center_freq - střední frekvence pro downlink
- ul_center_freq - střední frekvence pro uplink
- dl/ul_earfcn - kódové označení pro dvojici nosných vln, jedna pro uplink, druhá pro downlink, pomoci earfcn lze přímo nastavit použitou frekvenci
- dns_addr - IP adresa dns serveru, ve tvaru čtyř hexadecimálních parů hodnot
- ip_addr_start - první adresa IP poolu, přiřazuje se mobilním zařízením a TUN rozhraní
- mcc/mnc - kódy pro označení země a operátora v síti
- enable_pcap - umožňuje zaznamenávání IP komunikace do souboru (wireshark), pokud je tato možnost nastavena na 1, není možné sledovat real-time komunikaci přímo přes wireshark
- use_user/cnfg_file - ukládání uloženého nastavení do souboru, do tohoto souboru se neukládá hodnota tx_gain ani rx_gain a je nutné je po každém vypnutí OpenLTE zadat znovu, tyto soubory jsou uloženy ve složce /tmp

Hodnoty se mění syntaxí "write -parametr- hodnota" například "write dns_addr 08080808".

```
Radio Parameters:
        available_radios: (read-only)
                0: no_rf
                1: type=b200,name=,serial=F5D812,product=B210
        selected_radio_name (read-only) = type=b200,name=,serial=F5D812,product=B210
        selected_radio_idx = 1
        tx_gain = 86
        rx_gain = 35
        clock_source = internal
System Parameters:
        band = 20
        bandwidth = 5
        cell_id = 1
        debug_level = radio phy mac rlc pdcp rrc mme gw user rb timer iface msgq
        debug_type = warning info
        dl_center_freq = 806000000
        dl_earfcn = 6300
        dns_addr = 08080808
        enable_pcap = 1
        ip_addr_start = 0A000001
        mcc = 001
        mnc = 01
        n_ant = 1
        n_id_cell = 0
        p0_nominal_pucch = -96
        p0_nominal_pusch = -70
        q_hyst = 0
        q_rx_lev_min = -140
        search_win_size = 0
        sib3_present = 0
        sib4_present = 0
        sib5_present = 0
        sib6_present = 0
        sib7_present = 0
        sib8_present = 0
        tracking_area_code = 1
        ul_center_freq = 847000000
        ul_earfcn = 24300
        use_cnfg_file = 1
        use_user_file = 1
```

Obrázek 4.3: *Okno s konfiguračními údaji USRP a OpenLTE*

4.2.4 Přidání účastníka do databáze a konfigurace APN v mobilním zařízení

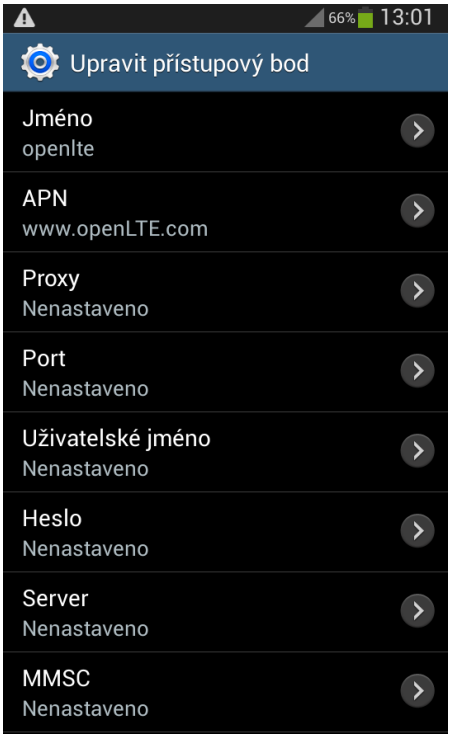
Dalšími příkazy, které slouží k přidání a výpisu uživatelů jsou:

- add_user imsi=<imsi> imei=<imei> k=<Ki> - přidá uživatele se zadanými parametry
- print_users - vypíše seznam uživatelů v databázi

Příkazem `add_user` je potřeba přidat do databáze uživatele podle vytvořené USIM karty a IMEI čísla mobilního zařízení. V mobilním zařízení, které budeme využívat, je nutné nastavit přístupový bod, což je možno provést pomoci konfigurace APN. Parametry APN by měly vypadat následovně:

- Jméno: openlte
- APN: www.openLTE.com
- APN protokol: IPv4
- APN roaming: IPv4

Zbytek údajů může zůstat nevyplněno, nebo může využít původně nastavené hodnoty. Také je vhodné v konfiguraci OpenLTE nastavit stejné MCC/MNC kódy jako jsou zapsané do USIM karty, tyto kódy tvoří prvních pět číslic IMSI, kvůli snazšímu nalezení OpenLTE sítě.

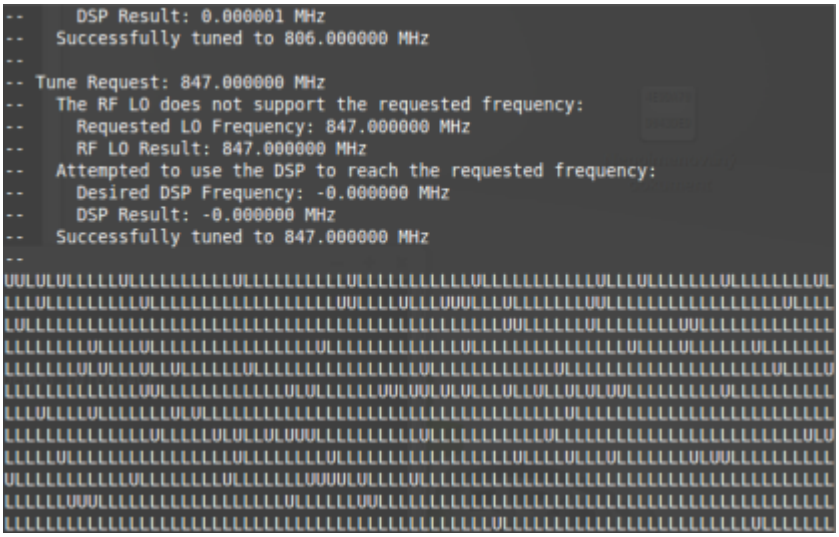


Obrázek 4.4: *Nastavení APN přístupového bodu v UE*

Nyní mimo konfigurace OpenLTE a UE zbývá nastavit vysílací a přijímací výkon pro samotné USRP. V testovacím prostředí stačí nastavit hodnotu `tx_gain` kolem 80, hodnotu *rx_gain* pak kolem 30. Při správné konfiguraci OpenLTE, UE a USRP s anténami, které mají zisk alespoň 5 dBi, by neměl být problém nalézt OpenLTE síť.

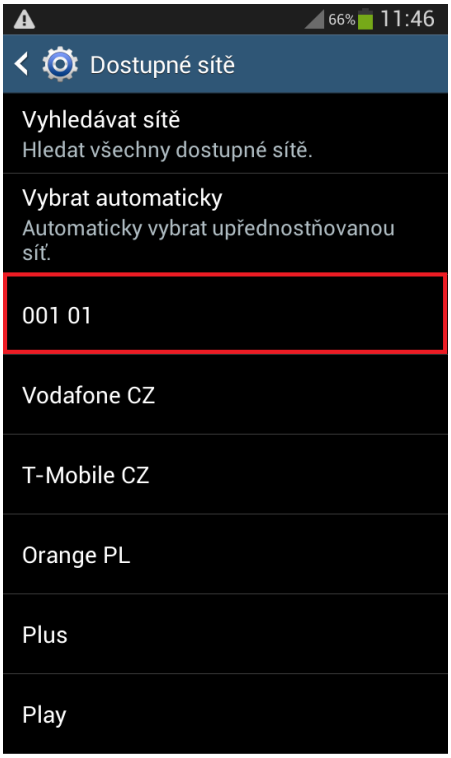
4.2.5 Spuštění OpenLTE sítě

Spuštění probíhá jednoduše, pokud jsou zadány všechny požadované konfigurační parametry, stačí spustit síť příkazem `start`. Poté by již mely být v hlavním okně OpenLTE viditelné zprávy, obsahující parametry USRP a následně i testovací vysílání dat, ve formátu U/L/O, kdy U znamená testovací upload zprávu a L symbolizuje download zprávu. Zpráva O charakterizuje, že došlo při přenosu testovací zprávy k chybě, většinou z důvodu špatné konfigurace OpenLTE nebo nedostatku systémových zdrojů.



Obrázek 4.5: *Hlavní okno OpenLTE po spuštění sítě s testovacími zprávami*

Dále je zde možnost sledovat logy a později po připojení UE do OpenLTE sítě i signalizační komunikaci mezi těmito prvky sítě. Tato komunikace je dostupná v okně, ve kterém je otevřená komunikace na portu 30001. Nyní zbývá se do OpenLTE sítě přihlásit z uživatelského UE. Síť bude pojmenována podle MCC/MNC kódů v nastavení OpenLTE, případně může být nazvána jako "PLMN 1-1", nebo i jinak, v závislosti na typu využitého mobilního zařízení.

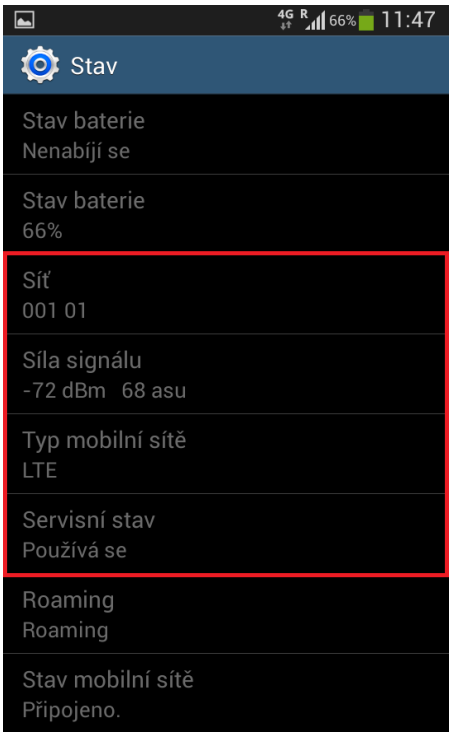


Obrázek 4.6: *Zobrazení OpenLTE sítě v UE Samsung Galaxy Core LTE*

Po vybrání této testovací sítě, by v konfiguračním okně měly byt zobrazeny zprávy o úspěšné autentizaci, zaregistrování UE do sítě a přiřazení tzv. default bearer, který slouží mimo jiné k přiřazení IP adresy mobilnímu zařízení.

```
start
ok
info user authentication successful imsi=1010000000108 imei=355676062567563
info user fully attached imsi=1010000000108 imei=355676062567563
info default bearer setup for imsi=1010000000108 imei=355676062567563
```

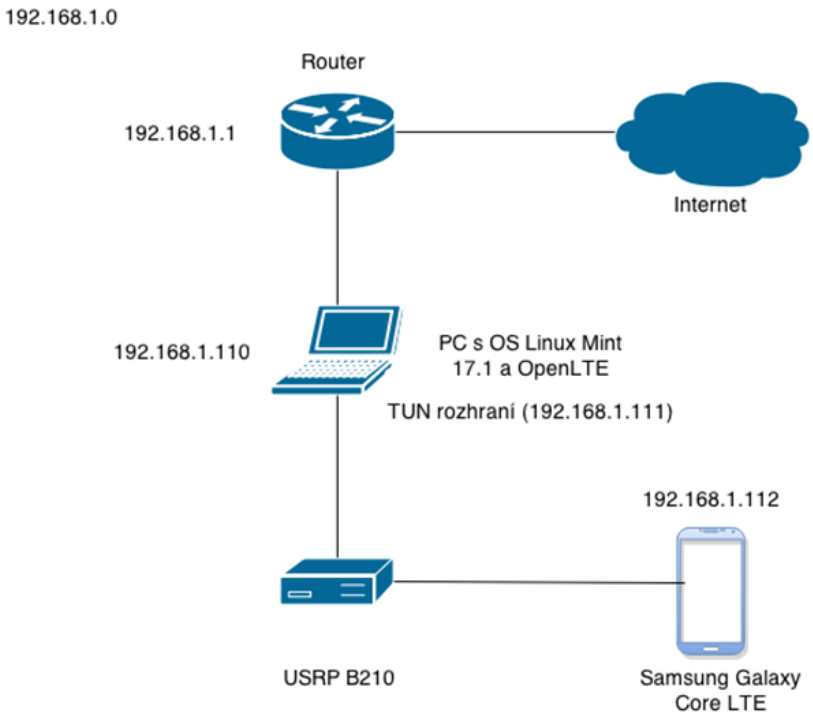
Obrázek 4.7: *Zprávy o úspěšné registraci zařízení do OpenLTE sítě*



Obrázek 4.8: *Údaje o OpenLTE síti v UE po registraci*

4.2.6 Analýza IP komunikace v OpenLTE síti

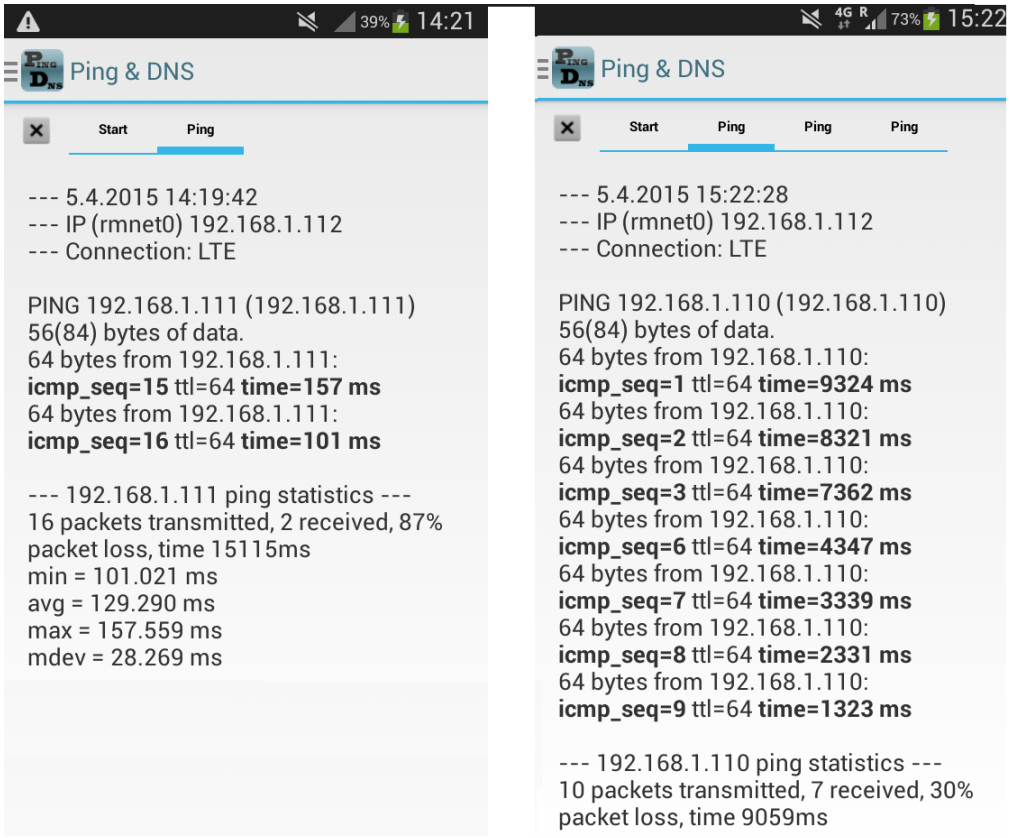
Pokud je mobilní zařízení úspěšně zaregistrováno v síti a je mu přiřazená IP adresa, je možné nyní otestovat funkčnost IP komunikace v síti OpenLTE. Jako paketový analyzér jsem využil aplikaci Wireshark, mobilní zařízení, pomoci kterého jsem testoval, byl mobilní telefon
Samsung Galaxy Core LTE. Testování probíhalo připojením přes domácí síť s jedním routerem, který směruje provoz do internetu. Podrobnější schéma celého experimentálního pracoviště je uvedeno na obrázku 4.9.



Obrázek 4.9: *Schéma experimentalního pracoviště*

Komunikace mezi mobilním zařízením a vnější sítí probíhá skrze TUN rozhraní, kterému je při spuštění OpenLTE sítě, stejně jako mobilnímu zařízení, přiřazena IP adresa podle nastavení `ip_addr_start` parametru. První z adres bude vždy přiřazena TUN rozhraní, poté následují adresy mobilních zařízení zaregistrovaných do OpenLTE sítě. Je důležité, aby IP adresy nekolidovaly s adresami ve vnitřní/domácí síti. Dále je potřeba ověřit, že se do iptables přidala pravidla určena pro forwarding paketů z TUN rozhraní na rozhraní, které využíváme pro připojení k internetu. To je možné zkontrolovat po zapnutí OpenLTE příkazem `iptables -L`. V případě, že by se zde pravidla pro rozhraní tun_openlte nevyskytovala, je možné upravit skript *enodeb_nat_script.sh* ve složce s OpenLTE instalačními soubory a poté skript znovu spustit.

Nejprve byla otestována vnitřní síť, tj. ping z mobilního zařízení na TUN rozhraní a následně na PC, na kterém běží OpenLTE. Jak lze vidět na obrázcích níže, ping na obě zařízení prošel, ovšem ve druhém případě, pingu na TUN rozhraní došlo k rozpadu spojení a pádu OpenLTE sítě. Dále je zde vidět velká odezva při pingu na PC, na kterém běží OpenLTE.



Obrázek 4.10: *Ping z mobilního zařízení na TUN zařízení (.111) a PC (.110)*

Následně proběhlo otestování dostupnosti připojení do internetu, zde byl použit program Wireshark k odchytu paketové komunikace.

Source	Destination	Protocol	Length	Info
192.168.1.112	208.67.222.222	DNS	68	Standard query 0x4e48 A 2.android.pool.ntp.org
208.67.222.222	192.168.1.112	DNS	132	Standard query response 0x4e48 A 81.27.192.20 A 92.62.233.2 A 91.216.168.42 A 80.79.25.111
192.168.1.112	208.67.222.222	DNS	61	Standard query 0xb55d A aloha.viber.com
208.67.222.222	192.168.1.112	DNS	240	Standard query response 0xb55d CNAME lb-684402412.us-east-1.elb.amazonaws.com A 174.129.234.
192.168.1.112	208.67.222.222	DNS	65	Standard query 0x0871 A play.googleapis.com
208.67.222.222	192.168.1.112	DNS	115	Standard query response 0x0871 CNAME googleapis.l.google.com A 216.58.211.10
192.168.1.112	208.67.222.222	DNS	60	Standard query 0xb25a A www.google.com
208.67.222.222	192.168.1.112	DNS	140	Standard query response 0xb25a A 173.194.116.243 A 173.194.116.240 A 173.194.116.242
192.168.1.112	208.67.220.220	DNS	61	Standard query 0xb55d A aloha.viber.com
208.67.220.220	192.168.1.112	DNS	240	Standard query response 0xb55d CNAME lb-684402412.us-east-1.elb.amazonaws.com A 50.16.205.12
192.168.1.112	208.67.222.222	DNS	77	Standard query 0xc355 A apchina-gld.push.samsungosp.com
208.67.222.222	192.168.1.112	DNS	174	Standard query response 0xc355 CNAME pan1elb-gld-615851265.ap-northeast-1.elb.amazonaws.com
192.168.1.112	208.67.220.220	DNS	60	Standard query 0xb25a A www.google.com
208.67.220.220	192.168.1.112	DNS	140	Standard query response 0xb25a A 173.194.116.243 A 173.194.116.242 A 173.194.116.244
192.168.1.112	208.67.222.222	DNS	65	Standard query 0x4043 A clients3.google.com
208.67.222.222	192.168.1.112	DNS	265	Standard query response 0x4043 CNAME clients.l.google.com A 173.194.116.232
192.168.1.112	208.67.220.220	DNS	77	Standard query 0xc355 A apchina-gld.push.samsungosp.com
192.168.1.112	208.67.220.220	ICMP	134	Destination unreachable (Port unreachable)
192.168.1.112	217.11.235.114	TCP	60	52867→80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=6147 TSecr=0 WS=64
217.11.235.114	192.168.1.112	TCP	64	80→52867 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1440 WS=1 TSval=0 TSecr=0 SACK_PERM=1
192.168.1.112	216.58.211.10	TCP	60	35523→443 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=6148 TSecr=0 WS=64
216.58.211.10	192.168.1.112	TCP	60	443→35523 [SYN, ACK] Seq=0 Ack=1 Win=42540 Len=0 MSS=1430 SACK_PERM=1 TSval=821367578 TSecr=
192.168.1.112	217.11.235.114	TCP	60	52868→80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=6170 TSecr=0 WS=64
217.11.235.114	192.168.1.112	TCP	64	80→52868 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1440 WS=1 TSval=0 TSecr=0 SACK_PERM=1
192.168.1.112	217.11.235.114	TCP	60	[TCP Spurious Retransmission] 52867→80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval
192.168.1.112	216.58.211.10	TCP	60	[TCP Spurious Retransmission] 35523→443 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSva
216.58.211.10	192.168.1.112	TCP	60	[TCP Retransmission] 443→35523 [SYN, ACK] Seq=0 Ack=1 Win=42540 Len=0 MSS=1430 SACK_PERM=1 TS
216.58.211.10	192.168.1.112	TCP	60	[TCP Retransmission] 443→35523 [SYN, ACK] Seq=0 Ack=1 Win=42540 Len=0 MSS=1430 SACK_PERM=1 TS
216.58.211.10	192.168.1.112	TCP	60	[TCP Retransmission] 443→35523 [SYN, ACK] Seq=0 Ack=1 Win=42540 Len=0 MSS=1430 SACK_PERM=1 TS
217.11.235.114	192.168.1.112	TCP	64	[TCP Retransmission] 80→52868 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1440 WS=1 TSval=0 TS
217.11.235.114	192.168.1.112	TCP	64	[TCP Retransmission] 80→52867 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1440 WS=1 TSval=0 TS
192.168.1.112	208.67.220.220	DNS	56	Standard query 0x57d6 A www.web.cz
208.67.220.220	192.168.1.112	DNS	72	Standard query response 0x57d6 A 217.11.235.114

Obrázek 4.11: *Zachycení paketové komunikace analyzérem Wireshark*

V první části jsou patrné hlavně DNS query pro nainstalované aplikace v mobilním zařízení jako je Google Play, Viber apod. Poté proběhl test připojení k webové stránce www.web.cz, ta byla zvolena kvůli svému minimalistickému vzhledu, aby nedocházelo k většímu množství přenesených dat. I přesto, že lze z Wiresharku vyčíst TCP komunikaci a DNS query pro tuto webovou stránku, nedošlo na mobilním zařízení k jejímu zobrazení. Z tohoto je patrné, že OpenLTE, která je ještě v alfa verzi, a IP komunikaci podporuje takřka čtyři měsíce, má zatím problémy s TCP protokolem. Tam, kde je využito UDP protokolu (DNS, DHCP...), probíhá komunikace relativně v pořádku. Co se tyče TCP protokolu, dochází zde k opakovanému nadbytečnému posílání stejné komunikace. Při TCP komunikaci také dochází k příchodu pouze částí jednotlivých celků paketů.

4.2.7 Analýza signalizačních zpráv OpenLTE

Další z možností využití, které OpenLTE nabízí je poměrně přehledné logování signalizační komunikace probíhající mezi UE a přístupovým bodem. Tyto zprávy je možné pozorovat na portu 30001.

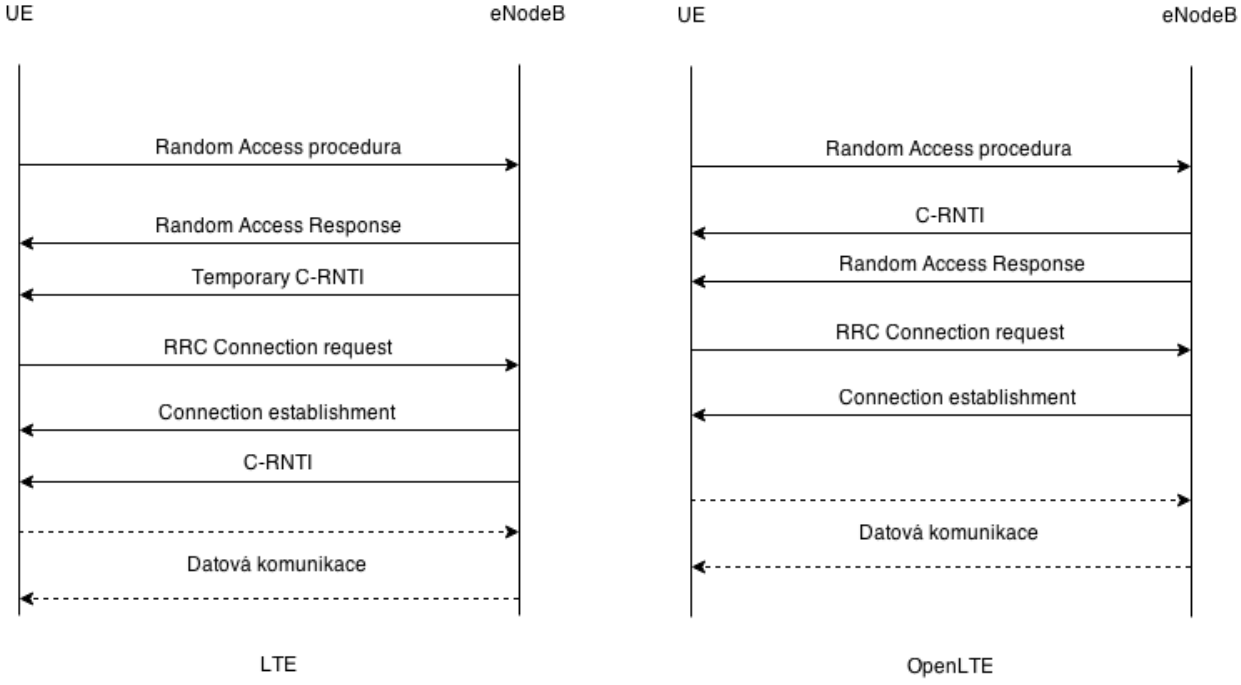
```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
04/10/2015 14:51:20.085399 info iface LTE_fdd_enb_interface.cc 768 *** LTE FDD ENB DEBUG INTERFACE ***
04/10/2015 14:53:10.635000 info user LTE_fdd_enb_user_mgr.cc 147 C-RNTI=61 assigned
04/10/2015 14:53:10.635158 info mac LTE_fdd_enb_mac.cc 851 RAR scheduled 1
04/10/2015 14:53:10.635655 info mac LTE_fdd_enb_mac.cc 978 RAR sent 9124 9131 9128 9134 400110640C003D
04/10/2015 14:53:10.636525 info phy LTE_fdd_enb_phy.cc 421 Received PDSCH schedule from MAC CURRENT_TTI:MAC=9128,PHY=9126 N_dl_allocs=1 N_ul_allocs=0
04/10/2015 14:53:10.645091 info phy LTE_fdd_enb_phy.cc 454 Received PUSCH schedule from MAC CURRENT_TTI:MAC=9134,PHY=9132 N_ul_decodes=1
04/10/2015 14:53:10.735049 info user LTE_fdd_enb_user_mgr.cc 147 C-RNTI=62 assigned
04/10/2015 14:53:10.735194 info mac LTE_fdd_enb_mac.cc 851 RAR scheduled 1
04/10/2015 14:53:10.735515 info mac LTE_fdd_enb_mac.cc 978 RAR sent 9224 9231 9228 9234 400110640C003E
04/10/2015 14:53:10.736312 info phy LTE_fdd_enb_phy.cc 421 Received PDSCH schedule from MAC CURRENT_TTI:MAC=9228,PHY=9226 N_dl_allocs=1 N_ul_allocs=0
04/10/2015 14:53:10.745233 info phy LTE_fdd_enb_phy.cc 454 Received PUSCH schedule from MAC CURRENT_TTI:MAC=9234,PHY=9232 N_ul_decodes=1
04/10/2015 14:53:10.748339 info mac LTE_fdd_enb_mac.cc 425 PUSCH decode for RNTI=62 CURRENT_TTI=9234 00506B8B0DBD46
04/10/2015 14:53:10.748448 info mac LTE_fdd_enb_mac.cc 595 Handling ULSCH SDU for RNTI=62, LCID=0 506B8B0DBD46
04/10/2015 14:53:10.748823 info rlc LTE_fdd_enb_rlc.cc 262 Received PDU for RNTI=62 and RB=SRB0 506B8B0DBD46
04/10/2015 14:53:10.749271 info pdcp LTE_fdd_enb_pdcp.cc 259 Received PDU for RNTI=62 and RB=SRB0 506B8B0DBD46
04/10/2015 14:53:10.749624 info rrc LTE_fdd_enb_rrc.cc 228 Received PDU for RNTI=62 and RB=SRB0 506B8B0DBD46
04/10/2015 14:53:10.749715 info rrc LTE_fdd_enb_rrc.cc 527 Received RRC Connection Request for RNTI=62, RB=SRB0
04/10/2015 14:53:10.749771 info rb LTE_fdd_enb_rb.cc 291 SRB0 RRC procedure moving from IDLE to RRC CON REQ for RNTI=62
04/10/2015 14:53:10.749821 info rb LTE_fdd_enb_rb.cc 310 SRB0 RRC state moving from IDLE to SRB1 SETUP for RNTI=62
04/10/2015 14:53:10.749872 info rrc LTE_fdd_enb_rrc.cc 883 Sending RRC Connection Setup for RNTI=62, RB=SRB0 60121B24080
04/10/2015 14:53:10.749972 info rb LTE_fdd_enb_rb.cc 291 SRB1 RRC procedure moving from IDLE to RRC CON REQ for RNTI=62
04/10/2015 14:53:10.750028 info rb LTE_fdd_enb_rb.cc 310 SRB1 RRC state moving from IDLE to WAIT FOR CON SETUP COMPLETE for RNTI=62
04/10/2015 14:53:10.750107 info pdcp LTE_fdd_enb_pdcp.cc 359 Received SDU for RNTI=62 and RB=SRB0 60121B24080
04/10/2015 14:53:10.750247 info pdcp LTE_fdd_enb_pdcp.cc 380 Sending PDU for RNTI=62 and RB=SRB0 60121B240800
04/10/2015 14:53:10.750579 info rlc LTE_fdd_enb_rlc.cc 579 Received SDU for RNTI=62 and RB=SRB0 60121B240800
04/10/2015 14:53:10.750657 info rlc LTE_fdd_enb_rlc.cc 627 Sending TMD PDU for RNTI=62, RB=SRB0 60121B240800
04/10/2015 14:53:10.750920 info mac LTE_fdd_enb_mac.cc 496 Received SDU for RNTI=62 and RB=SRB0 60121B240800
04/10/2015 14:53:10.751100 info mac LTE_fdd_enb_mac.cc 560 PDU scheduled for RNTI=62, DL_QUEUE_SIZE=1
04/10/2015 14:53:10.754582 info mac LTE_fdd_enb_mac.cc 1096 DL allocation (mcs=0, tbs=120, N_prb=5) sent for RNTI=62 CURRENT_TTI=9247 3F3C00506B8B0DBD
04/10/2015 14:53:10.755856 info phy LTE_fdd_enb_phy.cc 421 Received PDSCH schedule from MAC CURRENT_TTI:MAC=9247,PHY=9245 N_dl_allocs=1 N_ul_allocs=0
04/10/2015 14:53:10.769124 info mac LTE_fdd_enb_mac.cc 301 UL scheduled (mcs=0, tbs=208, N_prb=8) for RNTI=62, UL_QUEUE_SIZE=1
04/10/2015 14:53:10.769277 info mac LTE_fdd_enb_mac.cc 1168 UL allocation sent for RNTI=62 CURRENT_TTI=9266
04/10/2015 14:53:10.770263 info phy LTE_fdd_enb_phy.cc 421 Received PDSCH schedule from MAC CURRENT_TTI:MAC=9262,PHY=9260 N_dl_allocs=0 N_ul_allocs=1
```

Obrázek 4.12: *Zachycení signalizace mezi UE a eNodeB*

Na výše uvedeném obrázku je zachycená komunikace mezi mobilní stanicí, která se právě zaregistrovala do OpenLTE sítě a přístupovým bodem. V tomto konkrétním případě je UE přiřazená hodnota C-RNTI a eNodeB se snaží odeslat RAR odpověď na Preamble sekvenci, která byla poslána z mobilního zařízení směrem k eNodeB v rámci Random Access procedury, která slouží k prvotní identifikaci toho, že se do sítě snaží připojit nějaké mobilní zařízení. Tato RAR odpověď ovšem k UE nedojde, zřejmě v důsledku nízkého výkonu mobilního zařízení. Výkon tohoto zařízení je tedy zvýšen a celý cyklus se opakuje. Tentokrát již RAR odpověď k mobilnímu zařízení dorazí. Nyní jsou již využívány pro komunikaci sdílené kanály PDSCH a PUSCH a jsou vyhrazeny systémové zdroje pro

využití UL-SCH a DL-SCH mobilním zařízením. Zhruba v polovině logu (timestamp 749771) dochází k vyslání RRC requestu z mobilního zařízení a vydání odpovědi z eNodeB s parametry pro které RTNI je tato odpověď určena a který Radio Bearer bude využitý. Dále je zde zaznamenána vlastní datová komunikaci kdy dochází k příjmu SDU, jejich konverze na PDU a alokaci kanálů pro downlink a uplink. Zachycená komunikace je zde stejná, jako v případě odchycení pomoci Wiresharku a pravděpodobně se na posledních řádcích logu jedná o zachycení komunikace, některé ze služeb instalovaných v mobilním zařízení (Viber).

V prvních bodech tohoto logu je poměrně zřetelná odlišnost v použitých komunikačních kanálech mezi eNodeB a UE oproti typickému LTE. U LTE zprvu komunikuje UE s eNodeB pomoci sdíleného média a následně RA-RNTI (které je vypočítáno z timeslotu, ve kterém přišla Random Access zpráva od UE). Následně, po obdržení RAR potvrzení, je UE přiřazený tzv. dočasný C-RTNI identifikátor, přes který následně UE a eNodeB komunikují. Samotný C-RNTI identifikátor je určen až v posledním kroku schválení připojení k síti. Zde v OpenLTE probíhá přiřazení C-RNTI identifikátoru pro mobilní zařízení ihned v úvodu navázaní spojení, zřejmě proto, že se zatím nepočítá s větším množstvím připojených mobilních stanic na jednu instanci OpenLTE a tudíž je velmi nepravděpodobné, že by docházelo ke kolizím při Random Access proceduře.



Obrázek 4.13: *Rozdíl mezi LTE a OpenLTE při sestavování spojení s UE*

5 Zhodnocení dosažených výsledků

Pokud bych měl hodnotit výsledky, kterých jsem během psaní a experimentálního zkoumání této práce dosáhl, je nutné se zamyslet, z jakého pohledu je možné projekt jako je OpenLTE hodnotit. Pokud se bude jednat o uživatelskou přístupnost a náročnost toho, jakým způsobem je možné vytvořit základní experimentální pracoviště pro OpenLTE, tak zde by pro člověka, který má alespoň nějakou zkušenost s jakoukoliv linuxovou distribucí, neměl být problém. Pokud jde ovšem o *funkční* pracoviště, kde je možná pomoci mobilního zařízení komunikace s okolním prostředím pomoci této sítě, je nutné si nejdříve dobře promyslet, jaký hardware a software je pro takové pracoviště potřeba.

Co se týče mých testů, které jsem prováděl v této OpenLTE síti, tak musím konstatovat, že ačkoliv je projekt OpenLTE stále v alfa verzi a podporu pro IP komunikaci nabízí teprve od konce roku 2014, tak je schopný zprostředkovávat poměrně zajímavé výsledky právě v oné oblasti LTE IP komunikace, stejně jako v oblasti kontrolních a signalizačních zpráv, které probíhají v LTE sítích mezi mobilním zařízením a přístupovým bodem eNodeB.

Abych tedy shrnul výsledky IP komunikace, kterých se mi podařilo dosáhnout a kterých je verze OpenLTE 00.18.04, kterou jsem využil, vůbec schopná dosáhnout, tak se zde dá zatím hovořit o základní paketové komunikaci. Vyskytuje se zde poměrně zásadní problém s průchodem paketů ve směru z internetu k mobilnímu zařízení, který znemožňuje zobrazit na mobilním zařízení webový obsah. Některé pakety ovšem zachytit lze, a ty je pak možné paketovým analyzérem analyzovat. Například pingování z mobilního zařízení, dns query a obousměrnou komunikaci některých služeb nainstalovaných v mobilním zařízení (viber, google play...), které byly funkční téměř ve sto procentech případů. Za poměrně nefunkční lze zatím považovat TCP komunikaci, kdy dochází k opakovaným přenosům stejných paketů a pokud trvá spojení déle, může dojít až k destabilizaci celé OpenLTE sítě a následnému rozpadu spojení mezi OpenLTE a UE nebo dokonce pádu celého programu. Ovšem pokud vezmeme v úvahu, že tato funkcionalita je zde teprve několik měsíců, dá se hovořit o dobrých výsledcích.

Možnost sledovat signalizační zprávy pomoci konzole je v OpenLTE implementovaná už déle, a tak je možné sledovat celou řadu zpráv, které se při komunikaci vyskytují. I když se v některých krocích od běžné LTE sítě liší, nabízí možnost, jak se seznámit s tím, jak v jádru LTE síť funguje. Zde jsem nezaznamenal jediný problém.

Poslední částí, kterou bych chtěl zmínit, je poměrně velká nestabilita, která je dle mého názoru primárně zavíněna implementací využití IP komunikace. Po přihlášení UE do sítě a pouhém sledování a zaznamenávání logu byl program stabilní, pokud ale začala touto sítí proudit datová komunikace, tak se obvyklá doba provozu sítě pohybovala kolem tří až pěti minut, poté došlo k buď k pádu celého programu, odpojení UE od sítě nebo rovnou k chybě v USRP, které bylo třeba celé restartovat.

6 Závěr

Cílem této diplomové práce bylo vytvořit vlastní přístupový bod LTE eNodeB, pomoci softwarově definovaného rádia USRP B210 a open-source projektu OpenLTE. Dále pak zhodnotit funkčnost a případné využití tohoto přístupového bodu, do kterého bude zaregistrován účastník.

Nejprve tedy bylo nutné se seznámit s možnostmi rádia USRP B210, s ovládáním OpenLTE a také zjistit, co vše je potřebné pro to, aby bylo možné vlastní přístupový bod provozovat. Nejdříve bylo tedy potřeba prozkoumat využití rádiového spektra, aby nedošlo k narušení frekvencí ostatních operátorů a také aby bylo možné vlastní síť na mobilním zařízení nalézt, z důvodu pásem, které mobilní telefon podporuje. Dále pak musela byt splněna kritéria při výběru USIM karty, kterou je možné v OpenLTE síti použít. Protože nelze použít standardní USIM kartu operátorů České republiky, musela být naprogramována vlastní USIM karta s požadovanými parametry (IMSI, Ki...). Poté už mohl být účastník přidán do databáze OpenLTE sítě a po konfiguraci USRP, OpenLTE a mobilního telefonu, mohla být spuštěna síť, do které bylo možné se zaregistrovat a posléze začít testovat funkčnost samotného OpenLTE.

Tyto testy bych rozdělil do tří částí a to testování IP komunikace, analýza signalizačních zpráv a testování stability. IP komunikace byla implementována poměrně nedávno a nevykazuje tedy plnou funkčnost k tomu, aby bylo díky ní možné přenést větší množství dat nebo zobrazit na mobilním zařízení webovou stránku. Nabízí však možnost analýzy paketů v paketovém analyzátoru a poskytuje tak jakýsi náhled na to, kam by se mohl vývoj tohoto projektu dále ubírat a proč bude pravděpodobně za nějakou dobu více využíván – datový přenos.

Log, ze kterého je možné analyzovat signalizační zprávy, je plně funkční a poskytuje i člověku co nemá s LTE žádnou zkušenost se zde seznámit, jak funguje LTE síť ve svém jádru, protože podrobně popisuje komunikaci mezi přístupovým bodem eNodeB a mobilním zařízením. Zde také spatřuji v současnosti prozatím největší využití OpenLTE projektu, protože je možné využít rozbor signalizačních zpráv nejen k debuggingu a následnému zdokonalování tohoto projektu, ale také k podpoře výuky LTE sítí.

Co se týče stability, ta trpí nedostatky především kvůli nedávné implementace paketové komunikace a je při jejím využití velmi nestabilní. K rozpadu spojení dochází také i mimo využití IP komunikace, ovšem poměrně sporadicky a OpenLTE lze považovat za poměrně stabilní, bez větších problémů.

Jak už jsem zmínil, hlavní využití nyní vidím v použití OpenLTE jako pomůcky při výuce sítí LTE. Pokud bude vývoj projektu nadále pokračovat, určitě přibude i plně funkční IP komunikace a podpora VoLTE. V takovém případě, by mohl být projekt využit i jako částečná alternativa nebo

doplňující součást k současným, často využívaným projektům, jakými jsou například OpenBTS nebo OpenIMS.

V této diplomové práci jsem si rozšířil vědomosti, týkající se LTE sítí a seznámil se s projektem OpenLTE, kde jsem také využil vědomosti, nabyté při psaní mé bakalářské práce, která se týkala testování kvality hovorů v OpenBTS. Dále bylo velmi zajímavé spolupracovat s kolektivem, který se utvořil kolem projektu OpenLTE, kdy jsem na fóru, věnovanému tomuto projektu, mohl konzultovat své výsledky a případné problémy a společně je s touto komunitou řešit. Komunita, složená z přispěvatelů z celého světa, ovšem nemá v současné době mnoho členů a jsem tedy rád, že jsem mohl být jeden z prvních v České republice, který se tomuto tématu věnoval a získal tak cenné zkušenosti. Své zkušenosti s tímto projektem jsem také prezentoval na mezinárodním workshopu nazvaném Workshop on Advances Communication Technologies 2015, který se uskutečnil zde v Ostravě, v prostorách VŠB-TUO.

7 Seznam použité literatury

[1] BHALLA, Mudit Ratana a Anand Vardhan BHALLA. Generations of Mobile Wireless Technology: A Survey. *International Journal of Computer Applications* [online]. 2010-8-10, vol. 5, issue 4, s. 26-32 [cit. 2015-04-22]. DOI: 10.5120/905-1282. Dostupné z: http://www.ijcaonline.org/volume5/number4/pxc3871282.pdf

[2] Generations of Wireless Communication. (From 0G to 5G). *Generations of Wireless Communication. (From 0G to 5G)* [online]. 2008 [cit. 2015-04-22]. Dostupné z: http://www.scribd.com/doc/124320504/Generations-of-Wireless-Communication-From-0G-to-5G#scribd

[3] Generations of Network: 1G, 2G, 3G, 4G, 5G. [online]. 2009 [cit. 2015-04-22]. Dostupné z: http://www.slideshare.net/noorec786/generations-of-network-1-g-2g-3g-4g-5g

[4] The Telecom4U: Frequency Reuse. *The Telecom4U* [online]. 2013 [cit. 2015-04-22]. Dostupné z: http://thetelecom4u.blogspot.cz/2013/05/frequency-reuse.html

[5] GSM - Protocol Stack. *GSM - Protocol Stack* [online]. 2008 [cit. 2015-04-22]. Dostupné z: http://www.tutorialspoint.com/gsm/gsm_protocol_stack.htm

[6] 3G Systems WCD MA (UM TS) & Cdma2000. *3G Systems WCD MA (UM TS) & Cdma2000* [online]. 2005 [cit. 2015-04-22]. Dostupné z: https://upcommons.upc.edu/pfc/bitstream/2099.1/3590/2/36412-2.pdf

[7] MICHÁLEK, Libor. Rádiové sítě II, Systém UMTS Fyzická vrstva [online]. 2013

[8] CDMA2000. *CDMA2000* [online]. [cit. 2015-04-22]. Dostupné z: http://cs.wikipedia.org/wiki/CDMA2000

[9] *ARCHITEKTURA KANÁLŮ V SÍTÍCH UMTS*. Brno, 2008. Dostupné z: http://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=8963. Diplomová Práce. VUT.

[10] The USRP Board. *The USRP Board* [online]. 2005 [cit. 2015-04-22]. Dostupné z: http://homel.vsb.cz/~faj072/projekty/konvergence-openims-openbts/materialy/15_USRP_Board.pdf

[11] Ettus Research: A national instruments company. ETTUS RESEARCH. Http://www.ettus.com [online]. 2013 [cit. 2013-05-01]. Dostupné z: http://www.ettus.com

[12] LTE. *LTE* [online]. [cit. 2015-04-22]. Dostupné z: http://en.wikipedia.org/wiki/LTE_%28telecommunication%29

[13] MICHÁLEK, Libor. Rádiové sítě II, HSPA, LTE [online]. 2013

[14] M. Iedema. *Getting Started with OpenBTS.* O'Reilly, publishing scheduled on December 2014.

[15] A. Loula. *OpenBTS Installation and Configuration Guide.* 2009. Dostupné z:

http://gnuradio.org/redmine/attachments/139/OpenBTS_Guide_En_v0.1.pdf.

[16] S. Sesia, I. Toufik, M. Baker. *LTE - The UMTS Long Term Evolution: From Theory to Practice.* John Wiley & Sons, 2009. DOI: 10.1002/9780470742891